This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES.

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES.

BIBLIOTHECA BODLEIANA

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES.

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR GUILLAUME LIBRI.

PARIS.

IMPRIMERIE ROYALE.

—

1833.

181. h. 21.

premier degré par rapport à l'une des inconnues, et que M. Gauss a appelées *congruences*.

En partant de notre principe général, nous démontrons les théorèmes de Fermat et de Wilson, et beaucoup d'autres; puis nous établissons une formule qui renferme toute la théorie des congruences, et qui la ramène aux fonctions circulaires.

En considérant les congruences du premier degré, nous trouvons l'expression générale des racines de l'équation indéterminée du premier degré en fonction des coefficients (ce qui n'avait jamais été fait); et nous montrons qu'elles en sont une fonction trigonométrique. Ensuite, en passant aux congruences du second degré, nous retrouvons directement tous les théorèmes connus sur les résidus quadratiques.

Notre formule fondamentale, en établissant un rapport singulier entre les solutions des congruences et les fonctions circulaires, fournit le moyen de résoudre directement les équations à deux termes. M. Gauss, qui a découvert le premier cette résolution par une méthode très-ingénieuse, et Lagrange, qui l'a ensuite ramenée à sa théorie générale des équations, ont supposé que l'on connaissait toujours les racines primitives des nombres premiers. La méthode que nous exposons dans ce mémoire est indépendante de cette recherche, et d'ailleurs elle est beaucoup plus simple que celles qui ont été trouvées par ces deux grands géomètres, et qui exigent de très-longs calculs pour être mises en pratique.

On applique les mêmes principes aux congruences des ordres supérieurs, à la résolution des équations d'où dépend la division de la lemniscate en parties égales, et à beaucoup d'autres recherches : les exemples que nous avons choisis suffisent pour montrer de quelle manière notre méthode doit être modifiée dans les cas particuliers.

En partant des formules que nous donnons ici, nous avions trouvé précédemment une expression numérique de la somme des diviseurs d'un nombre quelconque : nous indiquons à présent une équation d'où l'on peut déduire la manière de trouver directe-

ment un nombre premier plus grand qu'une limite donnée. Mais comme cette recherche exigerait la connaissance de plusieurs formules que nous ne donnons pas à présent, nous nous réservons de résoudre complétement, dans une autre occasion, ce problème, qui a été considéré jusqu'ici comme très-difficile.

L'examen des formules que nous exposons dans cet essai montre qu'en général les fonctions numériques s'expriment par des séries, dont le nombre des termes et l'exposant de la variable augmentent avec la valeur de la variable elle-même, et qu'elles forment en conséquence un nouveau genre de transcendantes, qui ont des propriétés tout à fait différentes de celles déjà connues. Pour perfectionner notre théorie, il faut comparer ces transcendantes entre elles, et les réduire au plus petit nombre possible; mais cette recherche importante ne pouvait pas trouver place ici, et formera le sujet d'un travail particulier. Nous montrerons alors de quelle manière on peut abréger les calculs que notre méthode exige, en faisant usage des intégrales définies, et quelles sont les formes à choisir, afin d'en pouvoir calculer la valeur avec facilité. Le mémoire que nous avons l'honneur de présenter à l'Académie n'a pour but que de montrer de quelle manière on peut réduire la théorie des nombres à l'analyse ordinaire.

ANALYSE.

Nous avons avancé ailleurs pour la première fois que lorsqu'on avait une équation à plusieurs inconnues à résoudre en nombres entiers, le problème n'était indéterminé que parce qu'on négligeait d'en traduire en analyse toutes les conditions; et nous avons fait voir que, au contraire, on obtenait toujours un nombre d'équations qui surpassait de l'unité le nombre des inconnues; puisque étant proposée l'équation

$$\Phi(x, y, z, \ldots \text{ etc}) = 0;$$

pour exprimer que $x, y, z, \ldots$ etc., doivent être des nombres entiers, on avait les équations

$$\sin x\pi = 0, \quad \sin y\pi = 0, \quad \sin z\pi\ 0, \ldots \text{ etc.}$$

dont le nombre est égal à celui des inconnues.

Nous avons vu encore qu'étant proposée l'équation

$$\Phi(x, y, z, \ldots \text{etc.}) = 0,$$

le nombre de ses solutions entières et positives différentes de zéro était exprimé, à très-peu près, par la formule

$$\Sigma e^{-a(x+y+z\ldots\text{etc.})\overline{\varphi(x,y,z,\ldots\text{etc})}^2}$$

où il fallait intégrer entre les limites

$$x = y = z \ \ldots = 1,$$
$$x = y = z \ \ldots = \infty;$$

et nous avons donné des formules semblables pour d'autres fonctions numériques.

Lorsqu'on cherche seulement le nombre des solutions comprises dans la série

$$1, 2, 3, \ldots\ldots \text{A} - 1,$$

il suffit de considérer la formule

$$\Sigma e^{-a\overline{\varphi(x,y,z\ldots\text{etc.})}^2} \tag{1}$$

où il faut intégrer entre les limites

$$x = y = z \ \ldots = 1,$$
$$x = y = z \ \ldots = \text{A};$$

pourvu que a soit un nombre assez grand.

L'intégrale (1) ne peut pas s'obtenir en général; mais en développant en série par les puissances de a, comme la suite qui en

résulte est toujours convergente, on pourra la calculer directement, et l'on aura

$$\Sigma e^{-a\overline{\varphi(x,y,z\ldots\text{etc.})}^2} = \Sigma 1 - a\Sigma\overline{\varphi(x,y,z,\ldots\text{etc.})}^2 + \frac{a^2}{1.2}\Sigma\overline{\varphi(x,y,z,\ldots\text{etc.})}^4 - \text{etc.},$$

en intégrant par rapport à toutes les variables depuis l'unité jusqu'à la limite A.

On obtiendra de cette manière le nombre des solutions de l'équation

$$\varphi(x,y,z,\ldots\text{etc.}) = 0,$$

comprises dans la série des nombres

$$1, 2, 3, \ldots A - 1,$$

en calculant un nombre fini de termes; car comme on a toujours, pour des valeurs réelles de la variable

$$\Sigma X^{2n} < \Sigma (X^2)^n,$$

la série que nous considérons aura au numérateur un rapport d'un terme à l'autre plus petit que

$$1 : -a\Sigma\overline{\varphi(x,y,z,\ldots\text{etc.})}^2,$$

tandis que le dénominateur aura à chaque terme un facteur de plus, qui ira toujours en croissant; ce qui rendra la suite convergente.

L'intégrale (1) peut se développer assez simplement de la manière suivante.

Étant donnée l'équation

$$\varphi(z) = e_0 + e_1 z + e_2 z^2 + \ldots\ldots + e_n z^n + \text{etc.},$$

laquelle se réduit à

$$e^{uz} = 1 + uz + \frac{u^2z^2}{1.2} + \frac{u^3z^3}{1.2.3} + \ldots + \frac{u^nz^n}{1.2.3\ldots n} + \text{etc.}$$

lorsque $\Phi(z) = e^{uz}$, on aura dans ce cas

$$e_0 = 1, \quad e_1 = u, \quad e_2 = \frac{u^2}{1.2}, \ldots\ldots \quad e_n = \frac{u^n}{1.2.3..n}.$$

Si l'on fait à présent

$$(2) \quad \Sigma\Phi(z) = a_1 z + a_2 z^2 + a_3 z^3 \ldots\ldots + a_n z^n + \text{etc.}$$
$$\Sigma e^{uz} = b_1 z + b_2 z^2 + b_3 z^3 \ldots\ldots + b_n z^n + \text{etc.};$$

a_n sera une fonction du premier degré des coefficients

$$e_{n-1}, \quad e_n, \quad e_{n+1}, \text{ etc.},$$

et b_n sera une fonction semblable des coefficients

$$\frac{u^{n-1}}{1.2.3..(n-1)}, \quad \frac{u^n}{1.2.3....n}, \quad \frac{u^{n+1}}{1.2.3..(n+1)}, \text{ etc.};$$

de sorte que les diverses puissances de $u, u^2, \ldots\ldots u^n$, etc., resteront indépendantes entre elles, de même que les coefficiens $e_0, e_1, e_2, \ldots e_n$, et il ne pourra pas y avoir de réduction; de telle manière que si l'on a la valeur de b_n, on trouvera celle de a_n, en substituant partout dans la première

$$1.2.3....n e_n = \frac{d^n \varphi(z)}{dz^n},$$

(où il faut faire $z = 0$ après les différenciations), au lieu de u^n.

A présent l'on a

$$\Sigma e^{uz} = \frac{e^{uz} - 1}{e^z - 1},$$

et comme par les formules de M. Laplace, ou par celles que nous avons données dans les Mémoires de l'Académie de Turin (voyez la première note à la fin de ce mémoire), on peut trouver le développement de

$$\frac{1}{e^u - 1} = \frac{1}{u} + A_1 + A_2 u \ldots\ldots + A_n u^{n-1} + \text{etc.}$$

on aura

$$\Sigma e^{uz} = \left(\frac{1}{u} + A_1 + A_2 u + A_3 u^2 + \ldots + A_n u^{n-1} + \text{etc.}\right) \times$$

$$\times \left(uz + \frac{u^2 z^2}{1.2} + \frac{u^3 z^3}{1.2.3} \ldots + \frac{u^n z^n}{1.2.3..n} + \text{etc.}\right)$$

$$= b_1 z + b_2 z^2 + b_3 z^3 \ldots + b_n z^n + \text{etc.},$$

et par suite

$$b_n = \frac{u^{n-1}}{1.2.3..n} + \frac{A_1 u^n}{1.2.3..n} + \frac{A_2 u^{n+1}}{1.2.3..n} + \text{etc.}$$

Si l'on substitue dans cette équation $\frac{d^n \varphi(z)}{dz^n}$ au lieu de u^n, on aura en général

$$a_n = \frac{1}{1.2.3..n}\left(\frac{d^{n-1}\varphi(z)}{dz^{n-1}} + \frac{A_1 d^n \varphi(z)}{dz^n} + \frac{A_2 d^{n+1}\varphi(z)}{dz^{n+1}} + \text{etc.}\right)$$

On peut exprimer ce coefficient en termes finis de cette manière

$$a_n = \frac{1}{1.2.3..n}\left(\frac{\left(\frac{d\varphi(z)}{dz}\right)}{e^{\frac{d\varphi(z)}{dz}} - 1}\right),$$

pourvu qu'en développant on change $\frac{d\varphi(z)^p}{dz^p}$ en $\frac{d^p \varphi(z)}{dz^p}$, comme on le fait pour d'autres formules de la même espèce, et que l'on fasse $z = 0$ après les différenciations. En substituant les valeurs de

$$a_1, a_2, a_3, \ldots a_n,$$

exprimées de cette manière dans l'équation (2), on aura la formule

$$\Sigma\Phi(z) = \frac{z\frac{d\varphi(z)}{dz}}{dz\left(e^{\frac{d\varphi(z)}{dz}}-1\right)} + \frac{z^2}{1.2}\,\frac{\frac{d\varphi(z)^2}{dz^2}}{dz^2\left(e^{\frac{d\varphi(z)}{dz}}-1\right)} \cdots .$$

$$+ \frac{z^n}{1.2.3..n}\,\frac{\left(\frac{d\varphi(z)}{dz}\right)^n}{e^{\frac{d\varphi(z)}{dz}}-1} + \text{etc.} = \frac{e^{\frac{z\,d\varphi(z)}{dz}}-1}{e^{\frac{d\varphi(z)}{dz}}-1},$$

qui est assez simple.

Il faut observer ici que si l'on fait $\Phi(z) = e^{uz}$, on aura toujours

$$\frac{d\varphi(z)^n}{dz^n} = \frac{d^n\varphi(z)}{dz^n},$$

pourvu que l'on fasse $z = 0$ après les différenciations; c'est par cette raison que dans ce cas la formule

$$\frac{e^{\frac{z\,d\varphi(z)}{dz}}-1}{e^{\frac{d\varphi(z)}{dz}}-1} = \frac{e^{uz}-1}{e^u-1},$$

représente exactement la valeur de l'intégrale Σe^{uz}. On pourrait de la même manière développer $\Sigma^n\Phi(z)$, $\Delta^n\Phi(z)$, et en général

$$\Sigma^n.\ \Sigma'.\ \Sigma''.\ \ldots.\ \Phi(z, y, u, \ldots \text{etc.}),$$

les intégrations étant effectuées par rapport aux variables z, y, u, etc.

Les séries que l'on obtient de cette manière sont de peu d'utilité dans les applications numériques; car pour avoir une valeur approchée de l'intégrale (1), il faut calculer un nombre de termes qui croît avec la limite A de l'intégration, de telle manière qu'on obtient toujours une équation de degré indéfini, et qui est une fonction des coefficients de l'équation $\Phi(x, y, z, \ldots \text{etc.}) = 0$, et de la limite A. Mais il est à remarquer que les coefficients des variables x, y, z, etc., dans le développement de la fonction (1), sont

tels, qu'après un certain nombre de termes il s'opère une compensation, de manière qu'il ne reste à peu près que le nombre des solutions cherché. Cette considération, et l'examen attentif de la nature de ces coefficients, peuvent fournir une théorie complète des équations indéterminées; et déjà l'aperçu que nous avons indiqué suffirait pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire, mais nous allons reprendre plus généralement ce sujet.

Étant proposée une équation à plusieurs inconnues à résoudre en nombres rationnels (entiers ou fractionnaires), on pourra toujours la préparer de manière que tous les nombres qu'on cherche soient entiers et positifs, puisque, en général, si l'équation à résoudre était de la forme

$$\Phi(x, y, z, \ldots \text{ etc.}) = 0,$$

et qu'on cherchât pour $x, y, z,$ etc., des valeurs fractionnaires en faisant

$$x = \frac{x_1}{x_2}, \; y = \frac{y_1}{y_2}, \; z = \frac{z_1}{z_2}, \text{ etc.},$$

on aurait l'équation

$$\Phi\left(\frac{x_1}{x_2}, \; \frac{y_1}{y_2}, \; \frac{z_1}{z_2}, \text{ etc. }\right) = 0,$$

dans laquelle il ne faudrait chercher, pour $x_1, x_2, y_1, y_2,$ etc., que des valeurs entières; et d'ailleurs s'il y avait des solutions négatives, on les obtiendrait en changeant les signes des variables.

Soit donc proposée l'équation

$$\Phi(x, y, z, \ldots \text{ etc.}) = 0,$$

que nous représenterons pour abréger par $\Phi = 0$, à résoudre en nombres entiers et positifs : avec les méthodes connues on cherche à s'aider de la forme particulière des coefficients pour obtenir toutes les solutions. Mais l'équation $\Phi = 0$ exprime seulement les rela-

tions qui doivent exister entre les inconnues, et n'indique d'aucune manière qu'elles ne puissent recevoir que des valeurs entières. Cet oubli des conditions auxiliaires du problème a été la cause qu'il n'a pas été soumis à une analyse générale, parce qu'on ne le mettait pas en équation; et d'ailleurs c'est pour cela que l'on a appelé indéterminée l'équation $\Phi \equiv 0$, quoique souvent on trouvât qu'elle n'était pas résoluble; ce qui aurait dû faire soupçonner qu'il existait une équation de condition, laquelle n'étant pas satisfaite, le problème ne pouvait pas être résolu. Au reste la forme des racines des équations à une seule inconnue, et l'observation qui montrait que, dans celles à plusieurs inconnues, le nombre des racines était tout à fait indépendant du degré de l'équation proposée, auraient dû faire prévoir que cette équation de condition renfermait les coefficients de l'équation proposée, et les limites que l'on attribuait aux variables.

Nous allons considérer le problème *à priori*, et nous montrerons de quelle manière on peut trouver l'équation de condition, qui doit être satisfaite pour une équation quelconque; de manière que lorsque la limite des variables n'est pas l'infini, on pourra toujours trouver directement toutes les solutions de l'équation proposée.

Étant proposée l'équation à plusieurs inconnues

$$\Phi(x, y, z, \ldots \text{etc.}) = 0,$$

à résoudre en nombres entiers et positifs, supposons d'abord que l'on demande toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite a; à y des valeurs plus petites que b; à z des valeurs plus petites que c, et ainsi de suite; a, b, c, etc., étant des nombres entiers et positifs, on devra donc donner à x, y, z, etc., toutes les valeurs comprises dans les séries

$$\begin{aligned} x &= 0, 1, 2, 3, \ldots\ldots (a-1), \\ y &= 0, 1, 2, 3, \ldots\ldots (b-1), \\ z &= 0, 1, 2, 3, \ldots\ldots (c-1), \\ &\text{etc.}; \end{aligned}$$

et faire toutes les combinaisons possibles avec l'équation $\varphi = 0$. Ces valeurs seront comprises aussi dans les équations

$$X = x(x-1)(x-2) \ldots\ldots (x-[a-1]) = 0,$$
$$Y = y(y-1)(y-2) \ldots\ldots (y-(b-1]) = 0,$$
$$Z = z(z-1)(z-2) \ldots\ldots (z-[c-1]) = 0,$$
etc. ;

lesquelles expriment les conditions que, x soit un nombre entier positif et moindre que a, que y soit un nombre entier positif moindre que b, et ainsi de suite ; de manière que les équations

$$X = 0, \quad Y = 0, \quad Z = 0, \text{ etc.}, \quad \varphi(x, y, z, \ldots\ldots \text{etc}) = 0,$$

doivent exister ensemble, et déterminent entièrement le problème. Mais puisque le nombre de ces équations surpasse de l'unité celui des inconnues, en éliminant successivement x, y, z, etc., on parviendra à une équation de condition

$$F = 0,$$

qui comprendra seulement les limites a, b, c, etc., et les coefficients de l'équation $\varphi(x, y, z, \ldots\ldots \text{etc.}) = 0$, et qui devra être satisfaite, afin que l'équation proposée soit résoluble.

Lorsque l'équation de condition sera satisfaite, et qu'on sera certain par conséquent que l'équation

$$\varphi(x, y, z, \ldots\ldots) = 0$$

est résoluble, on reprendra l'une des équations à une seule inconnue, que nous avons obtenues par l'élimination avant de parvenir à l'équation $F = 0$: par exemple, une équation en x seule de la forme $X_1 = 0$, et en cherchant le plus grand diviseur commun entre $X = 0$ et $X_1 = 0$, on aura une équation en x de la forme $X_2 = 0$, dont toutes les solutions seront entières, et dont le degré exprimera le nombre des valeurs de x, qui satisfont à l'équation

$$\varphi(x, y, z, \ldots\ldots \text{etc.}) = 0 ;$$

et en résolvant l'équation $X_2 = 0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi(x, y, z, \ldots \text{ etc.}) = 0$. De même, si après l'élimination des autres $(n-1)$ inconnues, on parvient à une équation en y de la forme $Y_1 = 0$; en cherchant le plus grand commun diviseur entre $Y = 0$ et $Y_1 = 0$, et en l'égalant à zéro, on obtiendrait toutes les valeurs de y qui résolvent l'équation proposée; et l'on voit que la même chose aurait lieu relativement aux autres inconnues.

Il est clair que la même méthode pourrait s'appliquer à trouver directement toutes les solutions rationnelles de l'équation à une seule inconnue

$$ax^n + bx^{n-1} + cx^{n-2} \ldots + px + q = 0;$$

mais dans tous les cas cette méthode ne fournit que les racines inégales : cependant les racines égales peuvent être déterminées de la manière suivante.

Nous supposerons, pour simplifier le problème, qu'il s'agisse d'une équation à deux inconnues seulement, puisque la méthode est absolument la même lorsqu'il y en a un plus grand nombre.

Étant donnée l'équation

$$\varphi(x, y) = 0,$$

à résoudre en nombres rationnels; si à une valeur rationnelle de $y = b$, il en correspond n également rationnelles de $x = a$ (n étant plus grand que l'unité); en différenciant l'équation proposée par rapport à x, et cherchant le plus grand diviseur commun Δ entre

$$\frac{d.\varphi(x,y)}{dx}; \text{ et } \varphi(x, y),$$

on obtiendra $\Delta = \mathrm{F}(x, y)$, et il y aura un reste $\mathrm{R} = f(y)$, qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait donc $f(y) = 0$, on en déduira la valeur rationnelle de $y = b$, lorsque cette valeur existe : et substituant b pour y, on aura

$$\Delta = \mathrm{F}(x, b) = (x-a)^{n-1},$$

et on obtiendra les valeurs multiples de x que l'on cherchait.

Ce que nous avons dit dans l'hypothèse que n valeurs de $x = a$ correspondent à une valeur de $y = b$, s'applique aussi lorsqu'à une valeur de $x = \mathrm{A}$, il en correspond m de $y = \mathrm{B}$; pourvu que l'on change x en y, et que l'on effectue les opérations dans un ordre inverse.

Si R était zéro identiquement, nous aurions l'équation

$$\Delta = \mathrm{F}(x, y) = 0 = (x - \downarrow[y])^{m-1},$$

qui devrait exister en même temps que l'autre $\Phi(x, y) = 0$, et qui en serait un facteur : l'on ne pourrait donc pas déterminer la valeur de $y = b$; mais en divisant le polynome $\Phi(x, y)$ par Δ, le quotient Q contiendrait une seule des n racines de $x = \downarrow(y)$, et en cherchant le plus grand commun diviseur entre Δ et Q, on aurait l'équation $x - \downarrow(y) = 0$.

Nous avons supposé qu'il y avait seulement n valeurs de $x = a$, qui correspondaient à la valeur de $y = b$, mais si outre celle-là il y avait m valeurs de $x = c$, r valeurs de $x = e$, etc., il serait facile d'appliquer à ce cas la méthode déjà indiquée.

Soit proposée, par exemple, l'équation

$$x^2 - 2xy + 2y^3 - 1 = 0,$$

dans laquelle on veuille savoir si, parmi toutes les valeurs de y qui la résolvent, il y en a une égale à b, et telle qu'il lui en corresponde $n > 1$ de $x = a$: à cet effet on différenciera l'équation proposée par rapport à x, et l'on aura $x - y = 0$: puis en cherchant le plus grand commun diviseur entre ces deux équations, on aura $x - y$ pour quotient, et $2y^3 - y^2 - 1 = 0$ pour reste : et comme cette dernière équation est satisfaite en faisant $y = 1$; si l'on substitue cette valeur dans l'équation

$$x^2 - 2xy + 2y^3 - 1 = 0,$$

on aura

$$x^2 - 2x + 1 = (x - 1)^2 = 0 :$$

pour exprimer que $x, y, z, \ldots$ etc., doivent être des nombres entiers, on avait les équations

$$\sin x\pi = 0, \quad \sin y\pi = 0, \quad \sin z\pi\ 0, \ldots \text{ etc.}$$

dont le nombre est égal à celui des inconnues.

Nous avons vu encore qu'étant proposée l'équation

$$\Phi(x, y, z, \ldots \text{etc.}) = 0,$$

le nombre de ses solutions entières et positives différentes de zéro était exprimé, à très-peu près, par la formule

$$\Sigma e^{-a(x+y+z\ldots\text{etc.})\overline{\varphi(x,y,z,\ldots\text{etc})}^2}$$

où il fallait intégrer entre les limites

$$x = y = z \ \ldots\ = 1,$$
$$x = y = z \ \ldots\ = \infty;$$

et nous avons donné des formules semblables pour d'autres fonctions numériques.

Lorsqu'on cherche seulement le nombre des solutions comprises dans la série

$$1, 2, 3, \ldots\ A - 1,$$

il suffit de considérer la formule

$$\Sigma e^{-a\overline{\varphi(x,y,z\ldots\text{etc.})}^2} \tag{1}$$

où il faut intégrer entre les limites

$$x = y = z \ \ldots\ = 1,$$
$$x = y = z \ \ldots\ = A;$$

pourvu que a soit un nombre assez grand.

L'intégrale (1) ne peut pas s'obtenir en général; mais en développant en série par les puissances de a, comme la suite qui en

Étant proposée l'équation

$$(3) \qquad \varphi(x, y, z \ldots . \text{ etc.}) - pu = 0,$$

(dans laquelle, φ est une fonction quelconque des nombres entiers et positifs

$$x, y, z, \ldots . \text{ etc.},$$

p est un nombre entier quelconque, et u est un nombre entier positif ou négatif) il est clair d'abord que s'il existe des valeurs de $x, y, z, \ldots$ etc., qui résolvent l'équation proposée, et qui soient plus grandes que p, il y en aura aussi qui seront comprises entre zéro et p; ce seront ces dernières valeurs que nous considérerons toujours dans ce qui suit, à moins que nous n'indiquions spécialement le contraire.

A présent l'on sait que l'équation (3) équivaut à la congruence

$$\varphi(x, y, z, \ldots . \text{ etc.}) \equiv 0, \qquad [\text{mod.} p];$$

en supposant, pour simplifier le problème, que p soit un nombre premier, que cette congruence ne contienne que l'inconnue x, et qu'elle soit de la forme

$$X = x^m + Ax^{m-1} + Bx^{m-2} \ldots . Px + Q \equiv 0 \quad [\text{mod.} p],$$

si elle a une racine $x = a$, on pourra toujours la mettre sous la forme

$$(x - a) X_1 \equiv 0, \qquad [\text{mod.} p]$$

X_1 étant un polynome entier en x du degré $m - 1$: il résulte de là que la congruence $X \equiv 0$ [mod.p.] ne peut avoir que m racines, et que si elle a les m racines entières

$$a, b, c, d, e, f, \text{ etc.},$$

on pourra la mettre sous la forme

$$x^m + Ax^{m-1} + Bx^{m-2} \ldots . + Px + Q$$
$$\equiv (x-a)(x-b)(x-c)(x-d)(x-e)(x-f) \ldots \text{etc.} \quad [\text{mod.} p];$$

on aura alors les congruences (4)

$$a+b+c+d+e+f\ldots, \text{ etc.} \equiv -\mathrm{A}, \qquad [\text{mod.}\,p]$$

$$\left\{\begin{array}{r} ab+ac+ad\ \ldots\ +\text{etc.} \\ +bc+bd+be+\text{etc.} \\ +cd+ce+cf+\text{etc.} \\ \ldots\ldots\ldots\ldots+\text{etc.} \end{array}\right\} \equiv +\mathrm{B}, \qquad [\text{mod.}\,p]$$

$$\left\{\begin{array}{r} abc+abd+abe+\text{etc.} \\ +bcd+bce+bcf+\text{etc.} \\ +cde+cdf+\text{etc.} \\ \ldots\ldots\ldots\ldots\text{etc.} \end{array}\right\} \equiv -\mathrm{C}, \qquad [\text{mod.}\,p]$$

$$abcdef\ldots. \equiv \pm.\mathrm{Q}, \qquad [\text{mod.}\,p]$$

dans la dernière desquelles il faut prendre le signe + si m est pair, et le signe — si m est impair.

Pour trouver la somme des puissances r^{mes} des racines de cette congruence, on aura des formules semblables à celles que l'on obtient pour les équations, car en appelant

$$\mathrm{P}_r,\ \mathrm{P}_{r-1},\ \mathrm{P}_{r-2},\ \text{etc.},$$

la somme des puissances r^{mes}, $(r-1)^{mes}$, etc., de ces racines, on aura

$$\mathrm{P}_{r-1}+\mathrm{AP}_{r-1}+\mathrm{BP}_{r-2}\ \ldots\ +r\mathrm{R} \equiv 0, \quad [\text{mod.}\,p].$$

On peut de la même manière transformer les congruences, et en avoir les fonctions symétriques; en général quand on a trouvé une formule propre à représenter une fonction quelconque des racines de l'équation $\mathrm{X}=0$, si l'on suppose que la congruence de la même forme $\mathrm{X} \equiv 0 \quad [\text{mod.}\,p]$ ait toutes ses racines entières, on pourra trouver la même fonction des racines de la congruence exprimée par une formule semblable à celle que l'on a obtenue pour l'équation; de sorte que si $\Phi \equiv \mathrm{B}$ représente la fonction cher-

résulte est toujours convergente, on pourra la calculer directement, et l'on aura

$$\Sigma e^{-a\overline{\varphi(x,y,z\ldots\text{etc.})}^2} = \Sigma 1 - a\Sigma\overline{\Phi(x,y,z,\ldots\text{etc.})}^2 + \frac{a^2}{1.2}\Sigma\overline{\Phi(x,y,z,\ldots\text{etc.})}^4 - \text{etc.},$$

en intégrant par rapport à toutes les variables depuis l'unité jusqu'à la limite A.

On obtiendra de cette manière le nombre des solutions de l'équation

$$\Phi(x,y,z,\ldots\text{etc.}) = 0,$$

comprises dans la série des nombres

$$1, 2, 3, \ldots A-1,$$

en calculant un nombre fini de termes; car comme on a toujours, pour des valeurs réelles de la variable

$$\Sigma X^{2n} < \Sigma (X^2)^n,$$

la série que nous considérons aura au numérateur un rapport d'un terme à l'autre plus petit que

$$1 : -a\Sigma\overline{\Phi(x,y,z,\ldots\text{etc.})}^2,$$

tandis que le dénominateur aura à chaque terme un facteur de plus, qui ira toujours en croissant; ce qui rendra la suite convergente.

L'intégrale (1) peut se développer assez simplement de la manière suivante.

Étant donnée l'équation

$$\Phi(z) = e_0 + e_1 z + e_2 z^2 + \ldots + e_n z^n + \text{etc.},$$

laquelle se réduit à

$$e^{uz} = 1 + \ldots + \frac{u^3 z^3}{1.2.3} \ldots + \frac{u^n z^n}{1.2.3\ldots n} + \text{etc.}$$

que nous avons considérée précédemment, donne

$$A = 0,\ B = 0,\ \ldots.\ P = 0,\ Q = -1,$$
$$a = 1,\ b = 2,\ c = 3,\ d = 4,\ e = 5,\ f = 6, \text{ etc.}$$

$m = p - 1$ égal à un nombre pair: en substituant par conséquent les valeurs des racines a, b, c, d, e, f, etc., dans les congruences (4) on aura

$$1 + 2 + 3 \ldots\ldots + (p-1) \equiv 0, \qquad [\text{mod. } p]$$

$$\left\{\begin{array}{c} 1.2 + 1.3 \ldots. + 1(p-1) \\ + 2.3 + 2.4 \ldots. + 2(p-1) \\ \ldots. \text{ etc.} \end{array}\right\} \equiv 0, \qquad [\text{mod. } p]$$

$\ldots\ldots\ldots\ldots\ldots\ldots$ etc.,

$$\left\{\begin{array}{c} 1.2.3 + 1.2.4 + 1.2.5 + \text{etc.} \\ + 2,3.4 + 2.3.5 + 2.3.6 + \text{etc.} \\ + 3.4.5 + 3.4.6 + 3.4.7 + \text{etc.} \\ \ldots. \text{ etc.} \end{array}\right\} \equiv 0, \qquad [\text{mod. } p]$$

$\ldots\ldots\ldots\ldots\ldots\ldots$ etc.,

et enfin

$$1.2.3.4 \ldots. (p-1) + 1 \equiv 0, \qquad [\text{mod. } p]$$

Cette dernière congruence renferme le théorème de Wilson.

On démontrerait de la même manière tous les théorèmes que M. Gauss a insérés dans la troisième partie de ses Recherches arithmétiques, et beaucoup d'autres; par exemple, on obtient la congruence

$$1.2.3 \ldots. (g-1)(g+1) \ldots. (p-1) + g^{p-1} \equiv 0, \ [\text{mod. p.}]$$

qui est toujours vérifiée lorsque p est un nombre premier. De même on trouve que si p est un nombre premier, et que n ne soit pas divisible par $p - 1$, on aura

$$1^n + 2^n + 3^n \ldots. + (p-1)^n \equiv 0, \qquad [\text{mod. } p]$$

tandis que si n est un multiple de $(p-1)$ on obtiendra

$$1^n + 2^n + 3^n \ldots + (p-1)^n + 1 \equiv 0, \quad [\text{mod.}p]$$

Nous ne pouvons pas nous arrêter à développer les nombreuses conséquences qui dérivent de ce principe : cependant nous montrerons comment on peut retrouver et généraliser un théorème donné par M. Poinsot dans le Journal de l'école royale Polytechnique.

M. Poinsot a démontré que les racines de la congruence

$$x^n - 1 \equiv 0, \quad [\text{mod.}p]$$

dans laquelle $np+1$ est un nombre premier, se déduisent des racines de l'équation $x^n - 1 \equiv 0$, en ajoutant sous les radicaux compris dans l'expression de ces dernières, des multiples de $np+1$. Ce théorème est évident dans tous les cas.

En effet la congruence

$$x^n + Ax^{n-1} + Bx^{n-2} \ldots P x + Q \equiv 0, \quad [\text{mod.}a]$$

(dans laquelle a est un nombre quelconque) équivaut à l'équation

$$x^n + Ax^{n-1} + Bx^{n-2} \ldots + Px + (Q - ay) = 0,$$

dont les racines sont exprimées en général par la formule

$$x = \Phi(A, B, \ldots P, Q - ay),$$

qui se réduit à l'expression des racines de l'équation

$$x + Ax^{n-1} + Bx^{n-2} \ldots + Q = 0,$$

lorsqu'on y fait $y = 0$. Donc, *vice versâ*, si l'on ajoute des multiples de a sous les radicaux compris dans l'expression des racines de cette équation, on aura les racines de la congruence proposée.

En appliquant aux congruences ce que nous avons dit en général des équations indéterminées, on trouve que toutes les solutions de la congruence

$$\Phi(x, y, z, \ldots \text{etc.}) \equiv 0, \quad [\text{mod.}p]$$

et si ces facteurs sont en nombre pair, on pourra multiplier z par le facteur indéterminé $az_{n+1} - 1$, et l'on aura encore

$$Z(az_{n+1} - 1) \equiv aZ_1 - 1 \equiv 0, \qquad [\text{mod.}p].$$

D'où il résulte que la congruence

$$ax - 1 \equiv 0, \qquad [\text{mod.}p]$$

et par suite celle-ci

$$ax - b \equiv 0, \qquad [\text{mod.}p.]$$

est toujours résoluble, si a et p sont premiers entre eux.

L'on voit aisément que dans tous les cas une solution de la congruence proposée

$$ax - b \equiv 0, \qquad [\text{mod.}p_1.p_2.p_3 \ldots . p_n]$$

sera donnée par la formule

$$\frac{x}{b} = \frac{(a-1)(a^{p_1-1}-1)^2(a^{p_2-1}-1)^2 \ldots . (a^{p_n-1}-1)^2 + 1}{a},$$

qui exprimera l'une des racines de l'équation indéterminée

$$ax - b - py = 0.$$

Étant proposée la congruence

$$x^2 + 1 \equiv 0, \qquad [\text{mod. } 2p+1]$$

dans laquelle $2p+1$ est un nombre premier; pour savoir si elle est résoluble, on devra éliminer x entre celle-ci et l'autre

$$x^{2p} - 1 \equiv 0, \qquad [\text{mod. } 2p+1]$$

et l'on obtiendra la congruence de condition

$$(-1)^p - 1 \equiv 0, \qquad [\text{mod. } 2p+1]$$

qui sera toujours satisfaite lorsque p est pair, et qui sera im-

possible dans le cas contraire. On déduit de là ces deux théorèmes connus : 1° que la congruence

$$x^2 + 1 \equiv 0, \qquad [\text{mod. } 4p + 1]$$

est toujours résoluble ; 2° que l'autre

$$x^2 + 1 \equiv 0, \qquad [\text{mod. } 4p + 3]$$

ne l'est pas : $4p + 1$ et $4p + 3$ étant deux nombres premiers.

De même pour la congruence

$$x^a - b \equiv 0, \qquad [\text{mod. } ap + 1]$$

dans laquelle $ap + 1$ est un nombre premier, on aurait la congruence de condition $b^p - 1 \equiv 0$, [mod $ap + 1$], comme on le savait déjà.

On voit de là comment il faudrait opérer dans tous les cas ; mais il faut observer que puisque l'élimination entre les congruences se fait absolument de la même manière que pour les équations, étant proposées les congruences

$$\Phi(x, y, z \ldots \text{etc.}) \equiv 0, \qquad [\text{mod. } p]$$
$$x^p - x \equiv 0, \quad y^p - y \equiv 0, \quad z^p - z \equiv 0, \text{ etc. } [\text{mod. } p]$$

la congruence de condition s'obtiendra en éliminant toutes les inconnues entre les équations

$$\Phi(x, y, z, \ldots \text{etc.}) = 0, \tag{6}$$
$$x^p - x = 0, \quad y^p - y = 0, \quad z^p - z = 0, \text{etc.}$$

pourvu qu'au lieu de prendre l'équation de condition

$$F = 0,$$

qui en résulterait, on écrive

$$F \equiv 0, \qquad [\text{mod. } p.].$$

L'élimination entre les équations (6) peut s'effectuer avec les

méthodes connues, mais il faut observer qu'on obtiendra le même résultat si dans l'équation $\Phi(x, y, z, \ldots \text{etc.}) \equiv 0$, on substitue pour x, y, z, etc., leurs valeurs déduites des équations

$$(7) \qquad x^p - x \equiv 0, \quad y^p - y \equiv 0, \quad z^p - z \equiv 0, \text{ etc.}$$

en faisant le produit de tous les polynomes de la même forme dans lesquels on a substitué successivement pour x, y, z, etc., les racines des équations (7), et puisque ces racines sont connues, et que l'on a

$$x \equiv 0, \quad 1, \quad \cos\frac{2\pi}{p-1} + \sqrt{-1}\,\sin\frac{2\pi}{p-1}, \quad \text{etc.}$$

$$y \equiv 0, \quad 1, \quad \cos\frac{2\pi}{p-1} + \sqrt{-1}\,\sin\frac{2\pi}{p-1}, \quad \text{etc.}$$

la congruence de condition sera (voyez la note III à la fin de ce mémoire) :

$$\sum_{e} \log\left\{\Phi\left(e^{\frac{2x\pi\sqrt{-1}}{p-1}}, e^{\frac{2y\pi\sqrt{-1}}{p-1}}, e^{\frac{2z\pi\sqrt{-1}}{p-1}}, \ldots \text{etc.}\right)\right.$$

$$\left. \times \Phi\left(0, e^{\frac{2y\pi\sqrt{-1}}{p-1}}, e^{\frac{2z\pi\sqrt{-1}}{p-1}} \ldots \text{etc.}\right) \Phi\left(0, 0, e, e^{\frac{2z\pi\sqrt{-1}}{p-1}} \ldots \text{etc.}\right) \text{etc.}\right\}$$

$$\equiv 0, \qquad [\text{mod. } p]$$

en intégrant entre les limites

$$x = y = z, \ \ldots \text{etc.} = 0,$$
$$x = y = z, \ \ldots \text{etc.} = p-1,$$

Cette formule montre déjà de quelle manière, en appliquant notre théorie générale des équations indéterminées aux congruences, on les réduit à dépendre des fonctions circulaires.

On en pourrait déduire quelques-uns des théorèmes connus sur les congruences; mais il serait très-difficile de donner une théorie complète de ce genre d'équations, en partant de cette congruence

de condition, parce que sa forme ne permet pas d'effectuer les intégrations qu'elle exigerait pour être appliquée. Nous allons exposer une autre formule plus générale, qui nous fournira directement tous les théorèmes connus sur les congruences des différents degrés, et plusieurs propositions nouvelles.

Étant donnée l'équation à une seule inconnue

$$x^m - 1 = 0, \tag{8}$$

si l'on représente par

$$P_n, \quad P_{n-m}, \quad P_{n-2m}, \text{ etc.}$$

la somme des puissances

$$n^{mn}, \quad (n-m)^{mn}, \quad (n-2m)^{mn}, \text{ etc.}$$

on aura

$$P_n = P_{n-m} = P_{n-2m}, \ldots = P_{n-sm} \ldots \text{ etc.}$$

de sorte que si n est un multiple de m on obtiendra $P_n = m$, et dans le cas contraire on trouvera $P_n = 0$.

En exprimant les racines de l'équation (5) en fonctions circulaires, on aura

$$P_n = \left(\cos\frac{0\pi}{m} + \sqrt{-1}\sin\frac{0\pi}{m}\right)^n + \left(\cos\frac{2\pi}{m} + \sqrt{-1}\sin\frac{2\pi}{m}\right)^n \ldots + \left(\cos 2\frac{(m-1)}{m} + \sqrt{-1}\sin 2\frac{(m-1)}{m}\pi\right)^n,$$

et en réduisant les exposants à des multiples de l'arc, et négligeant les imaginaires, on obtiendra

$$P_n = \cos\frac{0n\pi}{m} + \cos\frac{2n\pi}{m} + \cos\frac{4n\pi}{m} \ldots + \cos 2\frac{(m-1)}{m}n\pi$$

$$= \sum_{s=0}^{s=m} \cos 2\frac{ns\pi}{m} = \frac{\sin 2\left(n - \frac{n}{2m}\right)\pi + \sin\frac{n\pi}{m}}{2\sin\frac{n\pi}{m}}$$

Il est clair, d'après ce que nous venons de dire, que si l'on prend

successivement la somme des puissances n^{mes}, des racines des équations

$$x - 1 = 0,\ x^2 - 1 = 0,\ x^3 - 1 = 0,\ \ldots\ x^m - 1 = 0 :$$

on aura la somme des diviseurs de n compris dans la série des nombres

$$1,\ 2,\ 3,\ 4\ldots\ldots\ m,$$

et qué pour avoir cette somme il faudra prendre l'intégrale

$$\Sigma\ \frac{\sin 2\left(n - \frac{n}{2\pi}\right)\pi\ +\ \sin\frac{n\pi}{x}}{2\ \sin\frac{nx}{x}}$$

entre les limites $x = 1$, $x = m + 1$; ou bien celle-ci $\Sigma \cos\ 2\frac{ny\pi}{x}$ entre les limites

$$y = 0,\quad y = x,\quad x = 1,\quad x = m + 1.$$

On trouverait de même que pour avoir le nombre des diviseurs de n compris dans la série des nombres

$$1, 2, 3, \ldots\ldots m;$$

il faut intégrer la formule $\Sigma\frac{1}{x}\cos\ 2\frac{ny\pi}{x}$ entre les limites

$$y = 0,\quad y = x,$$

$$x = 1,\quad x = m + 1.$$

Si l'on voulait la somme ou le nombre de tous les diviseurs de n; en représentant par $f(n)$ la première, et par $f\!\!\!\wedge(n)$ la seconde de ces fonctions, on aurait

$$\Sigma \cos 2\frac{ny\pi}{x} = f(n),$$

$$\Sigma \frac{1}{x} \cos 2\frac{ny\pi}{x} = \delta(n),$$

où il faut intégrer entre les limites

$$y = 0,\ y = x,\ x = 1,\ x = n + 1.$$

On sait que lorsque n est un nombre premier, on a

$$f(n) = n + 1,\quad \delta(n) = 2:$$

on aura par conséquent, en changeant les limites des intégrales, les deux équations

$$\Sigma \cos 2\frac{ny\pi}{x} = 1,\quad \Sigma \frac{1}{x} \cos 2\frac{ny\pi}{x} = 1,$$

(en intégrant entre les limites $y = 0$, $y = x$, $x = 1$, $x = n$) qui renferment deux propriétés spéciales des nombres premiers.

On a vu que n et m étant deux nombres entiers, la formule

$$(9) \qquad \frac{\sin 2\left(n - \frac{n}{2m}\right)\pi + \sin\frac{n\pi}{m}}{2\sin\frac{n\pi}{m}}$$

a pour valeur m, si n est divisible par m, et qu'elle se réduit à zéro si cette condition n'est pas remplie. Nous avons démontré de plus que p étant un nombre entier, l'expression

$$\frac{1.2.3.\ldots\ldots(p-1)+1}{p}$$

ne peut se réduire à un nombre entier que lorsque p est un nombre premier : en faisant donc

$$p = m;\quad 1.2.3.\ldots\ldots(p-1)+1 = n,$$

dans la formule (9) elle se transformera en celle-ci

$$\frac{\sin 2\left(1.2.3\ldots(p-1)+1-\frac{1.2.3\ldots(p-1)+1}{2p}\right)\pi+\sin\frac{(1.2.3\ldots(p-1)+1)\pi}{2p}}{2\sin\frac{(1.2.3\ldots(p-1)+1)\pi}{2p}}$$

qui devient p lorsque p est un nombre premier, et qui se réduit à zéro quand p est un nombre composé. Ainsi cette formule représente exclusivement tous les nombres premiers.

On pourrait varier beaucoup ces formules et les appliquer aux séries et à d'autres recherches, mais ce n'est pas ici le lieu de nous arrêter sur ce sujet.

Puisque la formule

$$\frac{1}{m}\left\{\left(\cos\frac{0\pi}{m}+\sqrt{-1}\,\frac{0\pi}{m}\right)^n+\left(\cos\frac{2\pi}{m}\sqrt{-1}\sin\frac{2\pi}{m}\right)^n\ldots.\right.$$
$$\left.+\left(\sin\frac{2(m-1)}{m}\pi+\sqrt{-1}\sin\frac{2\cdot(m-1)\pi}{m}\right)^n\right\}$$

a pour valeur l'unité ou zéro, selon que $\frac{n}{m}$ est un nombre entier ou fractionnaire, il s'ensuit que si l'on veut connaître le nombre des racines inégales de la congruence

$$\Phi(x, y, z, \ldots. \text{etc.}) \equiv 0, \qquad [\text{mod. } m]$$

dans laquelle on considère pour x, y, z, etc., les valeurs

$$\begin{aligned} x &= 0, 1, 2, 3 \ldots\ldots \quad (a-1), \\ y &= 0, 1, 2, 3, \ldots. \quad (b-1), \\ z &= 0, 1, 2, 3 \ldots\ldots \quad (c-1), \\ &\ldots\ldots \quad \text{etc.} \end{aligned}$$

il faudra intégrer la formule

$$\frac{1}{m}\Sigma\left\{\left(\cos\frac{0\pi}{m}+\sqrt{-1}\sin\frac{0\pi}{m}\right)^{\varphi(x,y,z\ldots\ldots\text{ etc.})}\right.$$
$$+\left(\cos\frac{2\pi}{m}+\sqrt{-1}\sin\frac{2\pi}{m}\right)^{\varphi(x,y,z\ldots\ldots\text{ etc.})}\quad\ldots\ldots$$
$$\left.+\left(\cos\frac{2(m-1)}{m}\pi+\sqrt{-1}\sin\frac{2(m-1)}{m}\pi\right)^{\varphi(x,y,z\ldots\ldots\text{ etc.})}\right\}$$

entre les limites

$$x=0,\ x=a;\ y=0,\ y=b;\ z=0,\ z=c;\ \text{etc.}$$

Cette formule est très-générale et peut servir, dans plusieurs cas, à déterminer sous forme finie la valeur de l'intégrale

$$\Sigma\, e^{a\varphi(x,y,z.\text{ etc.})\pi\sqrt{-1}}$$

comme nous le montrerons dans une autre occasion.

De même, la somme des racines de la congruence proposée sera exprimée par l'intégrale

$$\frac{1}{m}\Sigma\,(x,y,z\ldots\ldots\text{ etc.})\left\{\left(\cos\frac{0\pi}{m}+\sqrt{-1}\sin\frac{0\pi}{m}\right)^{\varphi(x,y,z\ldots\text{etc.})}\right.$$
$$+\left(\cos\frac{2\pi}{m}+\sqrt{-1}\sin\frac{2\pi}{m}\right)^{\varphi(x,y,z\ldots\ldots\text{ etc.})}\quad\ldots\ldots$$
$$\left.\left(\cos\frac{2(m-1)}{m}\pi+\sqrt{-1}\sin\frac{2(m-1)}{m}\pi\right)^{\varphi(x,y,z\ldots\ldots\text{ etc.})}\right\}$$

où il faudra intégrer entre les mêmes limites qu'auparavant.

On pourrait trouver beaucoup d'autres formules semblables, mais celles-ci sont suffisantes pour notre but : elles sont même trop générales, et il faudra les particulariser pour les appliquer avec facilité.

Nous observerons d'abord que, pour avoir toutes les solutions de la congruence

$$\Phi\,(x,y,z\ldots\ldots\text{ etc.})\equiv 0,\qquad [\text{mod. } m]$$

Il suffira de considérer celles qui sont comprises entre les limites

$$x = y = z \ldots\ldots = 0,$$
$$x = y = z \ldots\ldots = m,$$

puisque les autres s'en déduiront avec facilité; et ensuite que les imaginaires devant se détruire entre elles, on pourra considérer l'intégrale

$$10) \qquad N = \frac{1}{m}\Sigma\left\{\cos\frac{0\pi}{m} + \cos\frac{2\varphi(x,y,z\ldots\ldots\text{etc.})}{m}\pi \ldots\ldots + \cos 2\frac{(m-1)\varphi(x,y,z\ldots\ldots\text{etc.})\pi}{m}\right\}$$

prise entre les limites

$$x = y = z \ldots\ldots = 0,$$
$$x = y = z \ldots\ldots = m.$$

Si l'on veut, par exemple, le nombre des solutions entières et positives de l'équation

$$ax + b - cy = 0,$$

qui est équivalente à la congruence

$$ax \overset{\cdot}{+} b \equiv 0 \qquad [\text{mod. } c],$$

il faudra prendre l'intégrale

$$(11) \qquad \frac{1}{c}\Sigma\left\{\cos\frac{0\pi}{c} + \cos\frac{2(ax-b)\pi}{c} + \cos\frac{4(ax+b)\pi}{c} \ldots\ldots + \cos\frac{4(ax+b)\pi}{c} \ldots\ldots + \cos\frac{2(c-1)(ax+b)\pi}{c}\right\}$$

entre les limites

$$x = 0, \; x = c.$$

En considérant le terme général, on aura l'équation

$$\frac{1}{c}\Sigma \cos \frac{A(ax+b)\pi}{c}$$

$$= \frac{\sin \frac{A}{c}(b+ac-\frac{1}{2}a)\pi \quad -\sin \frac{A}{c}(b-\frac{1}{2}a)\pi}{2c \sin \frac{A}{2c}\pi}$$

dans le premier membre de laquelle le numérateur est toujours zéro, mais dont le dénominateur ne peut se réduire à zéro que lorsque a et c ont un diviseur commun plus grand que l'unité, puisque A est toujours plus petit que $2c$.

Il résulte de là que si a et c sont premiers entre eux, tous les termes de la formule (11) se détruiront, moins le premier dont la valeur se réduira à

$$\frac{1}{c}\sum_{x=0}^{x=c} \cos 0\, x\pi = \frac{c}{c} = 1.$$

Mais lorsque $a = mg$, $c = ng$, on fera $A = 2n$, et on obtiendra

$$\frac{1}{c}\sum_{x=0}^{x=c} \cos \frac{2n(ax+b)\pi}{c}$$

$$= \frac{\sin \frac{2n}{c}(b+ac-\frac{1}{2}a)\pi - \sin \frac{2n}{c}(b-\frac{1}{2}a)\pi}{2c \sin \frac{na\pi}{c}}$$

$$= \frac{\sin \frac{ba+ng-\frac{1}{2}a)\pi}{g} - \sin \frac{2(b-\frac{1}{2}a)\pi}{g}}{2c \sin \frac{a\pi}{g}}$$

Cette formule se réduit à $\frac{0}{0}$ lorsque $a = mg$; on devra donc différencier par rapport à a, pour en avoir la valeur déterminée, et on trouvera

$$\frac{1}{c}\sum_{x=0}^{x=c}\cos\frac{2n(b+ax)\pi}{c}$$

$$=\frac{2\left(ng-\frac{1}{2}\right)\frac{\pi}{g}\cos 2\left(b+nga-\frac{1}{2}a\right)\frac{\pi}{g}+\frac{\pi}{g}\cos\frac{2\left(b-\frac{1}{2}a\right)\pi}{g}}{\frac{2c\pi}{g}\cos\frac{a\pi}{g}}$$

$$=\frac{2\,ng\pi\cos\frac{2\left(b-\frac{1}{2}a\right)\pi}{g}}{2c\pi\cos a\frac{\pi}{g}}$$

$$=\frac{2\,c\pi\cos\frac{2b\pi}{g}.\cos m\pi+2c\pi\sin\frac{2b\pi}{g}\sin m\pi}{2c\pi\cos\frac{a\pi}{g}}=\cos\frac{2b\pi}{g}.$$

Mais puisque le nombre n est compris, $g-1$ fait dans $c-1$, la valeur de l'intégrale (11) sera (dans le cas que a et c aient un plus grand commun diviseur g) exprimée par la série

$$1+\cos\frac{2b\pi}{g}\cos\frac{4b\pi}{g}\ldots\ldots+\cos 2b\,\frac{(g-1)\pi}{g}$$

$$=\frac{\sin 2\left(b-\frac{1}{2}\frac{b}{g}\right)\pi+\sin\frac{b\pi}{g}}{2\sin\frac{b\pi}{g}}$$

dont la somme est égale à zéro, lorsque b n'est pas divisible par g, et qui a pour valeur g, lorsque $\frac{b}{g}$ est un nombre entier.

On tire de là

1° que la congruence

$$ax+b\equiv 0 \qquad [\text{mod. } c]$$

a toujours une solution positive, entière et plus petite que c, lorsque a et c n'ont d'autre commun diviseur que l'unité.

2° Que si a et c ont un commun diviseur g, qui ne divise point b, cette congruence ne pourra pas être résolue.

3° Que si $\frac{b}{g}$ est un nombre entier, on trouvera un nombre g de valeurs de x entières, positives, et plus petites que c, qui satisferont à la congruence proposée.

Il est clair que ces mêmes conditions s'appliquent à l'équation indéterminée

$$(12) \qquad ax + b - cy = 0.$$

On a déjà vu que l'intégrale indéfinie

$$\frac{1}{c}\Sigma x \left\{ \cos\frac{0\pi}{c} + \cos 2\frac{(ax+b)\pi}{c} + \cos 4\frac{(ax+b)\pi}{c} \ldots\ldots \right.$$
$$\left. + \cos 2A\frac{(ax+b)\pi}{c} \ldots\ldots + \cos 2\frac{(c-1)(ax+b)\pi}{c} \right\}$$

exprime la somme de toutes les valeurs entières et positives de x qui satisfont à la congruence

$$(13) \qquad ax + b \equiv 0, \qquad [\text{mod } c],$$

lorsqu'elle est résoluble, et que la valeur de l'intégrale (12) se réduit à zéro, si la congruence (13) n'est pas résoluble. En considérant le terme général

$$\frac{1}{c}\Sigma x \cos 2A\frac{(ax+b)\pi}{c}$$

on aura pour les formules connues d'intégration

$$(14) \qquad \Sigma x \cos 2A\frac{(ax+b)\pi}{c}$$
$$= \frac{(x-1)\sin 2A\frac{(ax+b-\frac{1}{2}a)\pi}{c} + \sin 2A\frac{(b-\frac{1}{2}a)}{c}\pi}{2c\sin 2A\frac{a\pi}{2c}}$$
$$+ \frac{\cos 2A\frac{(ax+b-a)\pi}{c} - \cos 2A\frac{(b-a)\pi}{c}}{c\left(2\sin 2\frac{Aa\pi}{2c}\right)^2}$$

et, pour avoir la somme des racines, il faudra intégrer cette formule depuis $A=0$, jusqu'à $A=c$.

A présent nous savons d'avance que si a et c ont un facteur commun qui ne divise point b, la congruence (13) n'est pas résoluble; et comme si ce facteur commun divise b aussi, on pourra toujours l'ôter, on supposera que a, b et c n'ont point de commun diviseur: alors, en donnant à A successivement toutes les valeurs

$$A = 0, 1, 2, 3 \ldots\ldots c - 1,$$

le premier terme se présenterait sous la forme $\frac{0}{0}$, et les autres auraient tous une valeur déterminée; mais pour éviter l'indétermination du premier terme, on l'intégrera séparément, et l'on aura

$$\frac{1}{c}\Sigma x \cos 0 \frac{(ax+b)\pi}{c} = \frac{1}{c}\Sigma x = \frac{c(c-1)}{2c}$$

et l'on intégrera entre les limites

$$A = 1, \; A = c;$$

cela peut se faire d'abord par les tables des sinus et cosinus, en calculant successivement les fonctions qui se rapportent aux valeurs

$$A = 1, \quad A = 2, \quad A = 3, \ldots\ldots \quad A = c - 1;$$

et l'on aura, de cette manière, résolu complétement le problème: mais, pour obtenir plus de généralité, on pourra, au moyen des expressions connues, transformer les cosinus et les sinus des multiples de l'arc en puissances des fonctions semblables de l'arc simple, et l'on aura une formule générale qui exprimera la somme cherchée.

Si l'on voulait la plus petite des solutions entières et positives de la congruence

$$ax + b \equiv 0, \qquad [\text{mod. } c]$$

il faudrait faire dans la formule (14) $x = c$, et elle deviendrait après les réductions

$$\frac{\sin \frac{2A}{c}(b - \frac{1}{2}a)\pi}{2 \sin \frac{Aa\pi}{c}}$$

et partant, la plus petite valeur de $x = \delta$, qui satisfait à la congruence proposée, sera donnée par la formule

$$\delta = \frac{c-1}{2} + \frac{1}{2} \sum_{u=1}^{u=c} \frac{\sin 2\left(b - \frac{1}{2}a\right)\frac{u\pi}{c}}{\sin \frac{au\pi}{c}}$$

et toutes les autres valeurs seront exprimées par la formule

$$x = \delta + cz,$$

dans laquelle z est un nombre entier quelconque.

Nous nous sommes arrêté sur ce problème, parce que les formules que nous avons trouvées offrent le premier exemple de l'expression analytique de la racine d'une équation indéterminée en fonction de ses coefficients. On sait qu'avec les méthodes connues on ne peut trouver les racines, même dans les cas les plus simples, que lorsque les coefficients sont donnés en nombre.

On pourrait multiplier beaucoup ces formules et en déduire la valeur finie de plusieurs intégrales définies aux différences et aux différentielles, assez difficiles à obtenir par d'autres voies; mais ce que nous avons dit ici suffit pour montrer l'esprit de notre méthode, et nous allons passer à des questions d'un ordre plus élevé. — Cependant, avant de traiter des congruences du second degré, nous indiquerons quelques propriétés élémentaires, déjà connues, des résidus quadratiques, que nous pourrions déduire de nos formules, mais dont, pour abréger, nous omettons la démonstration.

1° Si n est un nombre premier, en élevant successivement au carré tous les nombres

$$1,\ 2,\ 3 \ldots\ldots (n-1),$$

et divisant par n, on aura $\frac{n-1}{2}$, résidus quadratiques différents, répétés chacun deux fois, et il restera, dans la série des nombres naturels, $\frac{n-1}{2}$, nombres qui seront non-résidus.

2° Si l'on fait $n=2p+1$, et que l'on représente par

$$a_1,\ a_2,\ a_3,\ \ldots\ldots\ a_u,\ \ldots\ldots\ a_p,$$

les p résidus, et par

$$b_1,\ b_2,\ b_3,\ \ldots\ldots\ b_u,\ \ldots\ldots\ b_p,$$

les p non-résidus, on aura

$$\Sigma \cos \frac{2a_u\pi}{n} + \Sigma \cos \frac{2b_u\pi}{n} = \Sigma \cos \frac{2y\pi}{n},$$
$$\Sigma \cos \frac{2x^2\pi}{n} = 2\ \Sigma \cos \frac{2a_u\pi}{n},$$

en intégrant entre les limites

$$u=1,\ u=p+1;\ y=1,\ y=n;\ x=1,\ x=n.$$

En multipliant un résidu quelconque a_r par tous les autres, on aura la série

$$a_r\,a_1,\ a_r\,a_2,\ a_r\,a_3,\ \ldots\ldots\ a_r\,a_p,$$

qui donnera de nouveau tous les résidus disposés dans un autre ordre, et par conséquent l'on aura

$$\Sigma \cos \frac{2a_rx^2\pi}{n} = 2\Sigma \cos \frac{a_ra_u\pi}{n} = 2\Sigma \cos \frac{2a_u\pi}{n}.$$

En multipliant un résidu quelconque a_r par tous les non-résidus

$$b_1,\ b_2,\ b_n,\ \ldots\ldots\ b_p,$$

on aura de nouveau tous les non-résidus, d'où l'on déduira

$$\Sigma \cos \frac{2a_r b_u \pi}{n} = \Sigma \cos 2 \frac{b_u \pi}{n}.$$

En multipliant le non-résidu b_r par tous les autres, on aura tous les résidus, ce qui donnera

$$\Sigma \cos 2 \frac{b_r b_u \pi}{n} = \Sigma \cos 2 \frac{a_u \pi}{n}.$$

En multipliant enfin le non-résidu b_r par tous les résidus, on aura tous les non-résidus; ce qui fournira l'équation

$$\Sigma \cos 2 \frac{b_r a_u \pi}{n} = \Sigma \cos 2 \frac{b_u \pi}{n}.$$

Si on élève au carré tous les nombres

$$1, 2, 3, \ldots (n-1),$$

et qu'on les multiplie par un résidu quelconque a_r, on aura (en rejetant les multiples de n) la série des résidus

$$a_1,\ a_2,\ a_3,\ \ldots\ldots\ a_p$$

répétée deux fois, et par suite

$$\Sigma \cos 2 \frac{a_r\ x^2 \pi}{n} = 2 \Sigma \cos \frac{2a_u \pi}{n};$$

et si l'on multiplie ces $n-1$ carrés par un non-résidu quelconque b_p, on aura la série des non-résidus

$$b_1,\ b_2,\ b_n,\ \ldots\ldots\ b_p$$

répétée deux fois, d'où l'on tirera

$$\Sigma \cos \frac{2b_r x^2 \pi}{n} \equiv 2 \Sigma \cos \frac{2b_u \pi}{n}.$$

Dans toutes ces équations il faut intégrer entre les limites

$$u = 1, \quad u = p + 1, \quad x = 1, x = n,$$

et il est clair qu'elles subsisteraient de même si l'on changeait les cosinus en sinus.

Si l'on représente par N le nombre des solutions de la congruence

$$x^2 + c \equiv 0, \qquad [\text{mod. } n]$$

(et ce nombre par ce que nous avons dit ailleurs ne peut qu'être zéro ou deux), n étant toujours un nombre premier, on aura l'équation

$$n\,\mathrm{N} = \Sigma \cos 0 \left(\frac{x^2+c}{n}\right)\pi + \Sigma \cos 2\left(\frac{x^2+c}{n}\right)\pi + \Sigma \cos 4\left(\frac{x^2+c}{n}\right)\pi$$
$$\ldots. + \Sigma \cos 2\left(\frac{n-1}{n}\right)(x^2+c)\,\pi \equiv \Sigma \cos 2y\left(\frac{x^2+c}{n}\right)\pi$$

en intégrant entre les limites

$$x = 0, \quad x = n, \quad y = 0, \quad y = n,$$

ou bien celle-ci

$$n\,\mathrm{N} \equiv n + \Sigma \cos 2\frac{cy\pi}{n} + \Sigma \cos 2y\left(\frac{x^2+c}{n}\right)\pi$$

où il faut intégrer entre les limites

$$y = 1, \quad y = n, \quad x = 1, \quad x = n.$$

En développant les cosinus par les formules connues, on aura

$$n\,\mathrm{N} = n + \Sigma \cos 2\frac{cy\pi}{n}$$
$$+ \Sigma\left(\cos\frac{2yx^2}{n}\cos 2\frac{cy\pi}{n} - \sin 2\frac{yx^2\pi}{n}\sin\frac{2cy\pi}{n}\right).$$

A présent, il est clair, par ce que nous avons dit, que dans la valeur de cette intégrale on peut mettre au lieu de la série

$$1, 2, 3, \ldots\ldots n-1,$$

représentée par y, les deux autres

$$a_1, a_2, a_3, \ldots\ldots a_p; \quad b_1, b_2, b_3, \ldots\ldots b_p;$$

et l'on aura après la substitution

$$n\,\mathrm{N} = \Sigma\Big(\cos 2a_u x^2\pi \cos 2\frac{cu_u\pi}{n} + \cos 2\frac{b_u x^2\pi}{n} + \cos 2\frac{cb_u\pi}{n} - \sin 2\frac{a_u x^2\pi}{n}\sin 2\frac{cu_u\pi}{n} - \sin\frac{2b_u x^2\pi}{n}\sin\frac{2c_u\pi}{n}\Big) + n + \Sigma\cos\frac{2cy\pi}{n}$$

où il faudra intégrer entre les limites

$$x = 1,\ x = n,\ u = 1,\ u = p+1,\ y = 1,\ y = n.$$

En observant que

$$\sum_{y=1}^{y=n}\cos\frac{2y\pi}{n} = -1,$$

et en séparant les intégrales on obtiendra

$$n\,\mathrm{N} = \Sigma\Big(\cos 2\frac{ca_u\pi}{n}\,.\,\Sigma\cos 2\frac{a_u x^2\pi}{n}\Big) + \Sigma\Big(\cos 2\frac{cb_u\pi}{n}\,.\,\Sigma\cos 2b_u\frac{x^2\pi}{n}\Big) - \Sigma\Big(\sin 2\frac{cu_u\pi}{n}\,.\,\Sigma\sin 2\frac{a_u x^2\pi}{n}\Big) - \Sigma\Big(\sin 2\frac{cb_u\pi}{n}\,.\,\Sigma\sin 2\frac{b_u x^2\pi}{n}\Big) + n - 1,$$

ou il faudra intégrer d'abord entre les limites $x = 1$, $x = n$, et puis entre les limites $u = 1$, $u = p+1$.

A présent comme l'on a en général les équations

$$\Sigma \cos 2\frac{a_u x^2 \pi}{n} = 2\,\Sigma \cos 2\frac{a_u \pi}{n},$$
$$\Sigma \cos 2\frac{b_u x^2 \pi}{n} = 2\,\Sigma \cos 2\frac{b_u \pi}{n},$$

dans le premier membre desquelles il faut intégrer entre les limites

$$x = 1,\ x = n,$$

tandis que dans le second membre il faut intégrer entre les limites

$$u = 1,\ u = p + 1,$$

et que ces intégrales sont définies, elles deviendront égales à des constantes : la variable n disparaîtra, et on pourra les transporter en dehors du premier Σ. On aura alors, en répétant le même raisonnement pour les sinus,

$$(15)\quad \mathrm{N}\,n = 2\,\Sigma \cos 2\frac{ca_u\pi}{n}.\ \Sigma \cos 2\frac{a_u\pi}{n} + 2\,\Sigma \cos 2\frac{b_u\pi}{n}.\ \Sigma \cos 2\frac{cbu\pi}{n} - 2\,\Sigma \sin 2\frac{a_u\pi}{n}.\ \Sigma \sin 2\frac{ca_u\pi}{n} - 2\,\Sigma \sin\frac{2b_u\pi}{n}.\ \Sigma \sin 2\frac{ca_u\pi}{n} + n - 1,$$

et cette équation devra exister en même temps que les suivantes

$$(16)\quad \Sigma \cos 2\frac{a_u\pi}{n} + \Sigma \cos 2\frac{b_u\pi}{n} = \Sigma \cos\frac{2y\pi}{n} = -1,$$
$$\Sigma \sin 2\frac{a_u\pi}{n} + \Sigma \sin 2\frac{b_u\pi}{n} = \Sigma \sin\frac{2y\pi}{n} = 0,$$

en intégrant entre les limites

$$u = 1,\ u = p + 1,\ y = 1,\ y = n.$$

A présent supposons $c \equiv \pm 1$, $n \equiv 4m + 1$, et nous aurons deux solutions pour chacune des deux congruences

$$x^2 + 1 \equiv 0, \quad x^2 - 1 \equiv 0, \qquad [\text{mod. } n]$$

N sera égal à 2, et l'équation (15) se transformera en celle-ci

$$(17)\quad 2n = 2\left(\Sigma \cos 2\frac{a_u\pi}{n}\right)^2 + 2\left(\Sigma \cos 2\frac{b_u\pi}{n}\right)^2 \pm\left[\left(\Sigma \sin 2\frac{a_u\pi}{n}\right)^2 + 2\left(\Sigma \sin 2\frac{b_u\pi}{n}\right)^2\right] + n - 1,$$

d'où l'on tire, à cause du double signe,

$$\left(\Sigma \sin 2\frac{a_u\pi}{n}\right)^2 + \left(\Sigma \sin 2\frac{b_u\pi}{n}\right)^2 = 0,$$

$$n + 1 = 2\left(\Sigma \cos 2\frac{a_u\pi}{n}\right)^2 + 2\left(\Sigma \cos 2\frac{b_u\pi}{n}\right)^2,$$

et puisque l'on a

$$\left(\Sigma \cos 2\frac{b_u\pi}{n}\right)^2 = \left(\Sigma \cos 2\frac{a_u\pi}{n} + 1\right)^2,$$

l'équation (17) deviendra

$$n + 1 = 4\left(\Sigma \cos 2\frac{a_u\pi}{n}\right)^2 + 4\Sigma \cos 2\frac{a_u\pi}{n} + 2,$$

$$n = \left(2\Sigma \cos 2\frac{a_u\pi}{n} + 1\right)^2.$$

On tirera des équations précédentes

$$(18)\qquad \Sigma \cos 2\frac{a_u\pi}{n} = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n},$$

$$\Sigma \cos 2\frac{b_u\pi}{n} = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n},$$

$$\Sigma \sin \frac{a_u\pi}{n} = 0, \quad \Sigma \sin \frac{b_u\pi}{n} = 0.$$

Lorsque n est de la forme $4m + 3$, si l'on fait $c \equiv \pm 1$, la

congruence $x^2 - 1 \equiv 0 \,[\text{mod. } n]$ a deux solutions; mais l'autre $x^2 + 1 \equiv 0 \,[\text{mod. } n]$ n'est pas résoluble, alors on aura les deux équations

$$0 = n - 1 + 2\left(\Sigma \cos \frac{2a_u\pi}{n}\right)^2 + 2\left(\Sigma \cos 2\frac{b_u\pi}{n}\right)^2$$
$$- 2\left(\Sigma \sin 2\frac{a_u\pi}{n}\right)^2 - 2\left(\Sigma \sin 2\frac{b_u\pi}{n}\right)^2$$
$$2n = n - 1 + 2\left(\Sigma \cos 2\frac{a_u\pi}{n}\right)^2 + 2\left(\Sigma \cos 2\frac{b_u\pi}{n}\right)^2$$
$$+ 2\left(\Sigma \sin \frac{2a_u\pi}{n}\right)^2 + 2\left(\Sigma \sin 2\frac{d_u\pi}{n}\right)^2,$$

d'ou l'on déduira en les combinant avec les deux équations (16)

$$(18\,bis)\quad \Sigma \cos 2\frac{a_u\pi}{n} = -\tfrac{1}{2};\ \Sigma \sin \frac{2a_u\pi}{n} = \pm\tfrac{1}{2}\sqrt{n},$$
$$\Sigma \cos 2\frac{b_u\pi}{n} = -\tfrac{1}{2};\ \Sigma \sin \frac{2b_u\pi}{n} = \mp\tfrac{1}{2}\sqrt{n},$$

en intégrant partout entre les limites

$$u = 1,\ u = p + 1 = \frac{n-1}{2} + 1.$$

Ces sommations remarquables ont été données pour la première fois par M. Gauss dans ses Recherches arithmétiques, où il les a déduites de sa théorie de la division du cercle, et cet illustre auteur les a trouvées si intéressantes, qu'il a repris ce sujet dans un mémoire particulier pour les démontrer de nouveau. Mais les deux démonstrations que M. Gauss a données (les seules qui soient connues jusqu'à présent) sont très-longues et sont la conséquence des artifices particuliers dont cet illustre auteur s'est servi, sans dériver d'une méthode directe; au lieu que la manière dont nous y sommes parvenu est directe et très-générale, puisqu'elle peut conduire à beaucoup d'autres formules semblables. Cependant comme ces expressions renferment tout ce qu'on sait sur les congruences du second degré, nous allons reprendre, pour la simplifier, la démonstration que nous venons d'exposer.

Lorsque n est un nombre premier de la forme $4m + 1$, les deux congruences

$$x^2 + 1 \equiv 0, \quad x^2 - 1 \equiv 0, \qquad [\text{mod. } n]$$

seront résolubles et auront chacune deux solutions; alors on obtiendra l'équation

$$\begin{aligned}
2n = \Sigma \Big\{ &\Big(\cos\tfrac{0\pi}{n} + \sqrt{-1}\sin\tfrac{0\pi}{n}\Big)^{x^2 \pm 1} \\
&+ \Big(\cos\tfrac{2\pi}{n} + \sqrt{-1}\sin\tfrac{2\pi}{n}\Big)^{x^2 \pm 1} \ldots . \\
&\quad + \Big(\cos\tfrac{2t\pi}{n} + \sqrt{-1}\sin\tfrac{2t\pi}{n}\Big)^{x^2 \pm 1} \ldots . \\
&\quad\quad + \Big(\cos\tfrac{2(n-1)}{n}\pi + \sqrt{-1}\sin\tfrac{2(n-1)}{n}\pi\Big)^{x^2 \pm 1} \Big\} \\
= &\Big(\cos\tfrac{0\pi}{n} \pm \sqrt{-1}\sin\tfrac{0\pi}{n}\Big) \Sigma \Big(\cos\tfrac{0x^2\pi}{n} + \sqrt{-1}\sin\tfrac{0x^2\pi}{n}\Big) \\
&+ \Big(\cos\tfrac{2\pi}{n} \pm \sqrt{-1}\sin\tfrac{2\pi}{n}\Big) \Sigma \Big(\cos 2\tfrac{x^2\pi}{n} + \sqrt{-1}\sin 2\tfrac{x^2\pi}{n}\Big) \ldots . \\
&+ \Big(\cos 2\tfrac{t\pi}{n} \pm \sqrt{-1}\sin 2\tfrac{t\pi}{n}\Big) \Sigma \Big(\cos 2\tfrac{tx^2\pi}{n} + \sqrt{-1}\sin 2\tfrac{tx^2\pi}{n}\Big) \ldots . \\
&+ \Big(\cos 2\tfrac{(n-1)}{n}\pi + \sqrt{-1}\sin 2\tfrac{(n-1)}{n}\pi\Big) \times \\
&\times \Sigma \Big(\cos 2\tfrac{(n-1)}{n}(x^2 \pm 1)\pi + \sqrt{-1}\sin 2\tfrac{(n-1)}{n}(x^2 \pm 1)\pi\Big)
\end{aligned}$$

dans laquelle il faudra intégrer entre les limites $x = 0$, $x = n$.

A présent, si l'on effectue les multiplications indiquées et que l'on observe que les quantités imaginaires doivent se détruire entre elles, on trouvera

$$\begin{aligned}
2n = &\cos\tfrac{0\pi}{n} \Sigma \cos\tfrac{0x^2\pi}{n} + \cos\tfrac{2\pi}{n} \Sigma \cos 2\tfrac{x^2\pi}{n} \ldots . \\
&+ \cos 2\tfrac{t\pi}{n} \Sigma \cos 2\tfrac{tx^2\pi}{n} \ldots . + \cos 2\tfrac{(n-1)}{n}\pi \ \Sigma \cos 2\tfrac{(n-1)}{n}x^2\pi \\
&\mp \Big(\sin\tfrac{0\pi}{n} \ \Sigma \ \sin\tfrac{0x^2\pi}{n} + \sin\tfrac{2\pi}{n} \Sigma \sin 2\tfrac{x^2\pi}{n} \ldots . \\
&\quad + \sin 2\tfrac{t\pi}{n} \Sigma \sin 2\tfrac{tx^2\pi}{n} \ldots . + \sin 2\tfrac{(n-1)}{n} \Sigma \sin 2\tfrac{(n-1)}{n}x^2\pi\Big)
\end{aligned}$$

et par conséquent cette équation se décomposera dans les deux autres

$$2n = \cos\frac{0\pi}{n} \Sigma \cos\frac{0x^2\pi}{n} \ldots + \cos 2\frac{t\pi}{n} \Sigma \cos 2\frac{tx^2\pi}{n} \ldots$$

$$0 = \sin\frac{0\pi}{n} \Sigma \sin\frac{0x^2\pi}{n} \ldots + \sin 2\frac{t\pi}{n} \Sigma \sin 2\frac{tx^2\pi}{n} \ldots$$

Il faut observer ici qu'en laissant de côté le premier terme de chaque série, t doit prendre toutes les valeurs

$$1, 2, 3, \ldots\ldots n-1,$$

dont la moitié seront des résidus, et l'autre moitié des non-résidus : si l'on suppose $t = a_r =$ à un résidu quelconque, on aura

$$\cos 2\frac{t\pi}{n} \Sigma \cos 2\frac{tx^2\pi}{n} = \cos 2\frac{a_r\pi}{n} \Sigma \cos 2\frac{a_r x^2\pi}{n}$$

$$= \cos 2\frac{a_r\pi}{n} \Sigma \cos 2\frac{x^2\pi}{n};$$

et l'on aura de même, si t est un non-résidu b_r,

$$\cos 2\frac{b_r\pi}{n} \Sigma \cos 2\frac{b_r x^2\pi}{n} = \cos 2\frac{b_r\pi}{n}\left(1 + 2\Sigma \cos 2\frac{b_u\pi}{n}\right)$$

en intégrant entre les limites

$$x = 0,\ x = n,\ u = 1,\ u = 2m + 1 = p + 1;$$

on voit donc que la valeur de

$$\cos 2\frac{t\pi}{n} \Sigma \cos 2\frac{tx^2\pi}{n}$$

ne saurait être que l'une de celles-ci

$$\cos 2\frac{t\pi}{n}\left(1 + 2\Sigma \cos 2\frac{a_u\pi}{n}\right);\ \left(1 + 2\Sigma \cos 2\frac{b_u\pi}{n}\right)\cos 2\frac{t\pi}{n};$$

et qu'elle dépendra du nombre t; à présent comme parmi les nombres

$$1, 2, 3, \ldots\ldots n-1,$$

représentés par t, il y en a $\frac{n-1}{2}$ qui sont résidus et autant qui ne le sont pas, on pourra les réunir en deux groupes, et on obtiendra

$$2n = n + \left(1 + 2\Sigma\cos 2\frac{a_u\pi}{n}\right)\left(\cos 2\frac{a_1\pi}{n} + \cos 2\frac{a_2\pi}{n} \ldots + \cos 2\frac{a_p\pi}{n}\right)$$
$$+ \left(1 + 2\Sigma\cos 2\frac{b_u\pi}{n}\right)\left(\cos 2\frac{b_1\pi}{n} \ldots + \cos 2\frac{b_p\pi}{n}\right)$$
$$0 = 2\Sigma\cos 2\frac{a_u\pi}{n}\left(\sin 2\frac{a_1\pi}{n} + \sin 2\frac{a_2\pi}{n} \ldots + \sin 2\frac{a_p\pi}{n}\right)$$
$$+ 2\Sigma\sin 2\frac{b_u\pi}{n}\left(\sin 2\frac{a_1\pi}{n} \ldots + \sin 2\frac{a_u\pi}{n} + \text{etc.}\right),$$

et comme on a

$$\cos 2\frac{a_1\pi}{n} + \cos 2\frac{a_2\pi}{n} + \cos 2\frac{a_3\pi}{n} \ldots + \text{etc.} = \Sigma\cos 2\frac{a_u\pi}{n},$$
$$\cos 2\frac{b_1\pi}{n} + \cos 2\frac{b_2\pi}{n} + \cos 2\frac{b_3\pi}{n} \ldots + \text{etc.} = \Sigma\cos 2\frac{b_u\pi}{n},$$

on trouvera

$$2n = n + \left(\Sigma\cos 2\frac{a_u\pi}{n}\right)\left(1 + 2\Sigma\cos 2\frac{a_u\pi}{n}\right)$$
$$+ \left(\Sigma\sin 2\frac{b_u\pi}{n}\right)\left(1 + 2\Sigma\sin 2\frac{b_u\pi}{n}\right)$$
$$0 = 2\left(\Sigma\sin 2\frac{a_u\pi}{n}\right)^2 + 2\left(\Sigma\sin 2\frac{b_u\pi}{n}\right)^2$$

et si pour abréger on pose

$$\Sigma\cos 2\frac{a_u\pi}{n} = C,\ \Sigma\cos 2\frac{b_u\pi}{n} = C_n,$$
$$\Sigma\sin 2\frac{a_u\pi}{n} = S,\ \Sigma\sin 2\frac{b_u\pi}{n} = S_n,$$

on obtiendra

$$2n = n + C(2C + 1) + C_n(2C_n + 1)$$
$$0 = 2S^2 + 2S_n^2;$$

et puisque l'on a aussi

$$S + S_n = 0, \quad C + C_n = -1;$$

on déduira de ces quatre équations

$$C = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n}, \quad C_n = -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n},$$
$$S = 0, \quad S_n = 0.$$

Si n était de la forme $4m + 3$, on aurait les deux équations

$$2n = (1 + 2C)C + (1 + 2C_n)C_n + 2S^2 + 2S_n^2 + n,$$
$$0 = (1 + 2C)C + (1 + 2C_n)C_n - 2S^2 - 2S_n^2,$$

qui étant combinées avec les deux autres

$$C + C_n = -1, \quad S + S_n = 0,$$

donneraient

$$C = -\tfrac{1}{2}, \quad C_n = -\tfrac{1}{2}$$
$$S = \pm\tfrac{1}{2}\sqrt{n}, \quad S_n = \mp\tfrac{1}{2}\sqrt{n},$$

comme on l'avait déjà trouvé.

On voit de cette manière qu'étant proposée une congruence quelconque

$$x^2 + e \equiv 0, \qquad [\text{mod. } n]$$

le nombre n de ses solutions sera donné par la formule

$$(19)\quad N = \frac{1}{n}\left\{\begin{array}{c}(1+2C)\Sigma\cos 2\frac{ea_u\pi}{n} + (1+2C_n)\Sigma\cos 2\frac{eb_u\pi}{n} + n \\ -2S\,\Sigma\sin 2\frac{ea_u\pi}{n} - 2S_n\Sigma\sin 2\frac{eb_u\pi}{n}\end{array}\right\}$$

et comme $S = S_n = 0$ (lorsque n est un nombre premier de la forme $4m + 1$), on aura dans ce cas

$$N = \frac{1}{n}\left((1+2C)\Sigma\cos 2\frac{ea_u\pi}{n} + (1+2C_n)\Sigma\cos 2\frac{eb_u\pi}{n} + n\right)$$

et la valeur de N restera la même quand on changera $+e$ en $-e$, parce que dans cette expression il n'y a que des cosinus : donc si la congruence

$$x^2 + e \equiv 0 \qquad [\text{mod. } n]$$

est résoluble, celle-ci

$$x^2 - e \equiv 0 \qquad [\text{mod. } n]$$

le sera de même; et si la congruence

$$x^2 + e \equiv 0 \qquad [\text{mod. } n]$$

n'est pas résoluble, l'autre,

$$x^2 - e \equiv 0 \qquad [\text{mod. } n]$$

ne le sera pas non plus.

On voit que si n était de la forme $4m + 3$, la formule précédente (19) se réduirait à

$$n\,\mathrm{N} = -\left(2\mathrm{S}\,\Sigma \sin\frac{ea_u\pi}{n} + 2\mathrm{S}_u\Sigma\sin\frac{eb_u\pi}{n}\right) + n,$$

parce que dans ce cas on aurait

$$1 + 2\,\mathrm{C} = 0;\quad 1 + 2\,\mathrm{C}_u = 0;$$

et on tirerait de là, si e était un résidu,

$$n - (2\mathrm{S}^2 + 2\mathrm{S}_u^2) = n\,\mathrm{N} = n - \tfrac{1}{2}n - \tfrac{1}{2}n = 0;$$

et par suite $\mathrm{N} = 0$.

En supposant toujours que e est un résidu, et en changeant dans nos formules $+e$ en $-e$, on aurait

$$n\,\mathrm{N} = \tfrac{1}{2}n + \tfrac{1}{2}n + n = 2n,$$

$$\mathrm{N} = 2;$$

On déduit de là que si la congruence

$$x^2 + e \equiv 0 \qquad [\text{mod. } 4m+3]$$

est résoluble, l'autre,

$$x^2 - e \equiv 0 \pmod{4m+3},$$

ne le sera pas, *et vice versâ*.

Si l'on voulait connaître le nombre des racines de la congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{n},$$

n étant au nombre premier, et A et B étant deux nombres non divisibles par n, on aurait, en indiquant par N le nombre de ces solutions,

(20)

$$nN = \Sigma \begin{cases} 1 + \left(\cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}\right)^{x^2+Ay^2+B} \\ \ldots + \left(\cos\frac{2(n-1)}{n}\pi + \sqrt{-1}\sin\frac{2(n-1)}{n}\pi\right)^{x^2+Ay^2+B} \end{cases}$$

et la valeur de N dépendra des valeurs de A et de B. A présent, l'on peut supposer 1° que A et B sont deux résidus; 2° qu'ils sont tous les deux non résidus; 3° que A est résidu et B non résidu; 4° que A est non résidu, et B résidu : alors, en substituant dans l'équation (20) les valeurs trouvées précédemment, on aura les quatre équations qui correspondront aux quatre cas que nous avons considérés:

$$nN = n^2 + (1-1\pm\sqrt{\pm n})(1-\tfrac{1}{2}\pm\sqrt{\pm n})(-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{\pm n})$$
$$+(1-1\mp\sqrt{\pm n})(1-1\mp\sqrt{\pm n})(-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{\pm n}) = n^2 \pm n$$

$$nN = n^2 + (\pm\sqrt{\pm n})(\mp\sqrt{\pm n})(-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{\pm n})$$
$$+(\mp\sqrt{\pm n})(\pm\sqrt{\pm n})(-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{\pm n}) = n^2 \pm n$$

$$nN = n^2 + (\pm\sqrt{\pm n})\,(\pm\sqrt{\pm n})\,(\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{\pm n})$$
$$+(\mp\sqrt{\pm n})\,(\mp\sqrt{\pm n})\,(-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{\pm n}) = n^2 \pm n$$
$$n\,N = n^2 + (\pm\sqrt{\pm n})\,(\mp\sqrt{\pm n})\,(-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{+n}$$
$$+(\mp\sqrt{\pm n})\,(\pm\sqrt{\pm n}) + (-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{\pm n}) = n^2 \pm n.$$

On voit ici que N ne peut avoir que deux valeurs

$$N = n+1; \quad N = n-1:$$

et que par conséquent la congruence

$$x^2 + Ay^2 + B \equiv 0 \qquad [\text{mod. } n]$$

est toujours résoluble, lorsque n est un nombre premier. Lagrange, qui a démontré le premier ce théorème, n'a pas cependant déterminé le nombre des solutions comme nous l'avons fait. Cette proposition sert de base à la décomposition d'un nombre quelconque en quatre carrés, et l'on pourrait en déduire d'autres conséquences que nous sommes forcé de laisser de côté.

Nous avons vu que lorsque $n = 2p+1$ est un nombre premier de la forme $4m+1$, on a:

$$\Sigma\left(\cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}\right)^{a_u}$$
$$= \Sigma\cos 2\frac{a_u\pi}{n} + \sqrt{-1}\,\Sigma\sin 2\frac{a_u\pi}{n} = -\tfrac{1}{2}+\tfrac{1}{2}\sqrt{n};$$
$$\Sigma\left(\cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}\right)^{b_u}$$
$$= \Sigma\cos 2\frac{b_u\pi}{n} + \sqrt{-1}\,\Sigma\sin 2\frac{b_u\pi}{n} = -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n};$$

en intégrant entre les limites

$$u = 1, \quad u = 2m+1:$$

il résulte de là que si t est un nombre entier quelconque plus petit que n, on aura toujours

$$\Sigma\left(\cos 2\frac{t^2\pi}{n}+\sqrt{-1}\sin 2\frac{t^2\pi}{n}\right)^{a_u}=-\frac{1}{2}\pm\frac{1}{2}\sqrt{n},$$

$$\Sigma\left(\cos 2\frac{t^2\pi}{n}+\sqrt{-1}\sin 2\frac{t^2\pi}{n}\right)^{b_u}=-\frac{1}{2}\mp\frac{1}{2}\sqrt{n}.$$

Si l'on fait

$$\cos 2\frac{t^2\pi}{n}+\sqrt{-1}\sin 2\frac{t^2\pi}{n}=r^{t^2},$$

r exprimant la racine

$$x=\cos\frac{2\pi}{n}+\sqrt{-1}\sin\frac{2\pi}{n}$$

de l'équation

$$X=x^{n-1}+x^{n-2}\ldots\ldots+x^2+x+1=0,$$

on aura

$$X=x^{a_1}+x^{a_2}+x^{a_3}\ldots\ldots+x^{a_p}+\frac{1}{2}\mp\frac{1}{2}\sqrt{n}=0,$$

et cette équation, qui sera satisfaite par la valeur $x=r$, le sera aussi par toutes les valeurs

$$x=r^1,\ r^{2^2},\ r^{3^2},\ r^{4^2},\ \ldots\ldots\ r^{(n-1)^2},$$

qui se réduiront à la moitié, en négligeant les racines égales; et puisque ces mêmes racines résolvent l'équation $X=0$, elles seront communes aux deux équations

$$X=0,\ X_1=0.$$

Les autres racines qui résolvent l'équation $X=0$, outre celles que nous avons considérées, sont de la forme

$$r^{b_1},\ r^{b_2},\ r^{b_3}\ldots\ldots r^{b_p},$$

et ne peuvent pas résoudre l'équation $X_1=0$; car en y substituant l'une quelconque d'entre elles, comme l'on a en général $r^{ba_u}=r^{b_t}$, on trouvera

$$r^{b_1}+r^{b_2}\ldots\ldots+r^{b_p}+\frac{1}{2}\mp\frac{1}{2}\sqrt{n}=0,$$

équation absurde, puisque l'on a déjà eu

$$r^{b_1}+r^{b_2}\ldots\ldots+r^{b_p}+\frac{1}{2}\pm\frac{1}{2}\sqrt{n}=0;$$

donc les deux équations $X=0$, $X_{,}=0$, auront seulement les p racines communes,

$$r^{a_1},\ r^{a_2},\ r^{a_3},\ \ldots\ldots\ r^{a_p};$$

et en cherchant le plus grand diviseur commun Δ entre X et $X_{,}$, on aura une équation du degré $p=\frac{n-1}{2}$ qui contiendra toutes les racines de la forme $x=r^{a_u}$, a_u étant un résidu quelconque, tandis que l'équation $\frac{X}{\Delta}=\Delta_1=0$, comprendra toutes les racines de la forme $x=r^{b_u}$, b_u étant un non résidu quelconque.

Cette manière d'opérer la décomposition de l'équation $\frac{x^n-1}{x-1}=0$, est directe et beaucoup plus simple que celle proposée par M. Gauss : on verra dans la suite qu'elle peut s'étendre à tous les cas en général.

Il faut observer ici que lorsque $n=4m+1$, les coefficients des diverses puissances de x dans l'équation $\Delta=0$, seront fonctions en général de $-\frac{1}{2}\pm\frac{1}{2}\sqrt{n}$; tandis que les coefficients des mêmes puissances dans l'équation $\Delta_1=0$, seront des fonctions semblables de $-\frac{1}{2}\mp\frac{1}{2}\sqrt{n}$. Cela est évident, car si l'on fait

$$\Delta=x^p+A_1x^{p-1}+A_2x^{p-2}\ldots\ldots=A_p+0,$$
$$\Delta_{,}=x^p+B_1x^{p-1}+B_2x^{p-2}\ldots\ldots=B_p+0,$$

et que l'on appelle P_r la somme des puissances r^{mes} des racines de l'équation $\Delta=0$, et P'_r la somme des puissances r^{mes} des racines de l'équation $\Delta_1=0$, on aura toujours, lorsque r n'est pas un multiple de n,

$$P_r=-\tfrac{1}{2}\pm\tfrac{r}{2}\sqrt{n},$$
$$P_r+P'_r=-1:$$

et il n'y aura par conséquent entre P_r et P'_r d'autre différence que dans le signe de $\sqrt{n}$; toutes les autres choses étant les mêmes : donc si l'on suppose

$$\Delta=X_2+Y_2\sqrt{n}$$

on aura

$$\Delta_1 = X_2 - Y_2 \sqrt{n},$$

et par conséquent,

$$X = \Delta\Delta_1 = X_2^2 - n Y_2^2.$$

On trouvera de la même manière que, si n est de la forme $4m + 3$, on obtient

$$X = X_2^2 + n Y_2^2$$

et on aura en général, lorsque n est un nombre premier,

$$\frac{x^n - 1}{x - 1} = X_2^2 \pm n Y_2^2,$$

X_2 et Y_2 étant des fonctions rationnelles de x.

En égalant les coefficients des mêmes puissances de x dans l'équation

$$\left(x^p + \left(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{\pm n}\right) x^{p-1} + \left(\frac{a}{b} + \frac{c}{d}\sqrt{\pm n}\right) x^{p-2} + \text{etc.}\right)$$
$$\left(x^p + \left(\tfrac{1}{2} - \tfrac{1}{2}\sqrt{\pm n}\right) x^{p-1} + \left(\frac{a}{b} - \frac{c}{d}\sqrt{\pm n}\right) x^{p-2} + \text{etc.}\right)$$
$$= x^{n-1} + x^{n-2} \ldots\ldots + x^2 + x + 1 = 0,$$

on trouvera aisément que les coefficients numériques des deux facteurs

$$X_2 + Y_2 \sqrt{+n}, \quad X_2 - Y_2 \sqrt{\pm n},$$

ne peuvent admettre d'autre dénominateur que le nombre 2, d'où l'on déduira l'équation

$$4 \left(\frac{x^n - 1}{x - 1}\right) = X_2^2 \pm n Y_2^2 = 0,$$

qui aura toujours lieu lorsque n est un nombre premier, et dans laquelle X_2 et Y_2 seront des polynomes entiers en x, à coefficients entiers. Ce théorème a été découvert par M. Gauss, qui l'a déduit de sa théorie des équations à deux termes; il sert à prou-

ver que l'équation $\frac{x^n-1}{x-1}=0$ peut toujours se décomposer en deux autres du degré $\frac{n-1}{2}$, lorsque n est au nombre premier.

Pour appliquer ce théorème à la théorie des congruences, nous observerons que, d'après ce que nous avons démontré, si n est un nombre premier de la forme $ar+1$, la congruence

$$x^a - 1 \equiv 0 \qquad [\text{mod. } n]$$

aura toujours a solutions; et comme si a est un nombre premier impair, on a aussi

$$4\,(x^a-1) = (x-1)\,(Z^2 \pm aU^2),$$

il s'ensuit que $\pm a$ est résidu quadratique de $ar-1$, où il faut prendre le signe $+$, si a est de la forme $4m+1$, et le signe $-$, si a est de la forme $4m+3$.

Nous avons trouvé

$$\sum_{x=1}^{x=n} r^{x^2} = -1 \pm \sqrt{n} \text{ lorsque } n = 4m+1,$$

$$\sum_{x=1}^{x=n} r^{x^2} = -1 \pm \sqrt{-n} \text{ lorsque } n = 4m+3;$$

on pourrait déterminer le signe du radical, et l'on trouverait que l'on doit toujours prendre le signe positif, comme M. Gauss l'a fait dans les mémoires de Gottingue; mais cette démonstration nous écarterait trop de notre but, et nous la supprimerons.

Puisqu'on a

$$Y^2 \pm n\,Z^2 = 4\,X,$$

Si l'on rejette les multiples de n, on trouvera

$$Y \equiv 2\sqrt{X} \equiv 2\sqrt{\frac{x^n-1}{x-1}} \qquad [\text{mod. } n]$$

et puisque $n = 2p+1$, on aura

$$Y \equiv 2\sqrt{\frac{x^{2p+1}-1}{x-1}} \equiv 2\sqrt{x^{2p}\left(1-\frac{1}{x}\right)^{-1}\left(1-\frac{1}{x^{2p+1}}\right)}$$

$$\equiv 2x^p\sqrt{\left(1-\frac{1}{x}\right)^{-1}\left(1-\frac{1}{x^{2p+1}}\right)}; \quad [\text{mod. } p]$$

Mais comme on n'a besoin que des puissances positives de x, et plus petites que p, on pourra négliger le facteur

$$\left(1-\frac{1}{x^{2p+1}}\right)^{\frac{1}{2}},$$

et on obtiendra

$$(21) \qquad Y \equiv 2x^p\left(1-\frac{1}{x}\right)^{-\frac{1}{2}} \equiv 2x^p + x^{p-1} + \frac{3}{4}x^{p-2}$$

$$+\frac{3.5}{4.6}x^{p-3} + \frac{3.5.7}{4.6.8}x^{p-4} + \text{etc.}, \qquad [\text{mod. } p]$$

où il faudra rétablir au numérateur des multiples de n, qui rendent entiers tous les coefficients. On déduira aisément de là la valeur de Z, puisque l'on a

$$nZ^2 = Y^2 - 4X.$$

A présent il faut observer que dans les deux facteurs

$$(Y + Z\sqrt{+n})\ (Y - Z\sqrt{+n})$$

il y en a toujours un qui a pour racines tous les termes de la forme

$$x = \cos 2\frac{a_n\pi}{n} + \sqrt{-1}\sin 2\frac{a_n\pi}{n},$$

tandis que dans l'autre on a

$$x = \cos 2\frac{b_n\pi}{n} + \sqrt{-1}\sin 2\frac{b_n\pi}{n},$$

et que l'on aura toujours

$$\Sigma\left(\cos 2\frac{a_u\pi}{n}+\sqrt{-1}\sin 2\frac{a_u\pi}{n}\right)=-\frac{1}{2}+\frac{1}{2}\sqrt{\pm n},$$

$$\Sigma\left(\cos 2\frac{b_u\pi}{n}+\sqrt{-1}\sin 2\frac{b_u\pi}{n}\right)=-\frac{1}{2}-\frac{1}{2}\sqrt{\pm n},$$

où il faudra prendre le signe supérieur, si $n=4m+1$, et l'inférieur, si $n=4m+3$.

La méthode que nous avons exposée pour trouver les coefficients numériques de l'équation

$$\tfrac{1}{2}\,Y\pm\tfrac{1}{2}\,Z\sqrt{\pm n}=0,$$

est indépendante de toute considération sur le nombre n, en tant qu'il est ou n'est pas diviseur de $t^a\pm a$; si l'on ordonne donc l'équation

$$\tfrac{1}{2}\,Y\pm\tfrac{1}{2}\,Z\sqrt{\pm n}=0$$

par les puissances descendantes de x, on pourra, par les formules connues, trouver la somme des puissances de ses racines, les coefficients étant donnés : alors il faudra observer que si l'on appelle P_a la somme des puissances a^{mes} des racines de cette équation, on aura en général $P_a=P_1$, si a est un résidu quadratique de n, et $P_a=1-P_1$, si a est non résidu. On pourra donc reconnaître directement de cette manière si a est ou n'est pas résidu de n.

L'équation (10) dont nous sommes partis, qui établit un rapport si remarquable entre les intégrales aux différences des fonctions circulaires et le nombre des solutions d'une congruence, peut donner directement la résolution des équations à deux termes, que M. Gauss a trouvée le premier, en partant de considérations particulières, et en s'appuyant sur la connaissance des racines primitives.

Lagrange, qui depuis a repris cette matière, en partant des formules générales qu'il avait données précédemment, suppose aussi que l'on connaisse ces racines primitives. Nous avons simplifié cette résolution en la rendant indépendante de la recherche de ces racines, et en la déduisant d'une seule formule.

Nous allons ici énoncer quelques propositions qui nous seront

nécessaires à cet effet; mais nous en supprimerons les démonstrations, parce qu'elles nous écarteraient trop de notre but, et que d'ailleurs il est facile d'y suppléer.

Supposons que $an + 1$ soit un nombre premier quelconque, et que l'on élève successivement à la puissance a tous les nombres

$$1, 2, 3\ 4, \ldots\ldots\ an;$$

Si l'on divise toutes ces puissances par $an + 1$, on obtiendra n résidus divers entre eux, et plus petits que $an + 1$, qui seront chacun répétés a fois.

Si l'on appelle

$$A_1,\ A_2,\ A_3, \ldots\ldots \qquad A_n,$$

les résidus trouvés de cette manière, en multipliant l'un quelconque A_p d'entre eux, par la suite des puissances a^{mes}:

$$1^a,\ 2^a,\ 3^a, \ldots\ldots \qquad (an)^a,$$

on obtiendra de nouveau la série des nombres

$$A_1,\ A_2,\ A_3, \ldots\ldots \qquad A_n,$$

situés dans un ordre quelconque, et répétés chacun a fois: l'on aura par conséquent

$$\Sigma \cos 2\frac{x^a\pi}{an+1} = 1 + a\,\Sigma \cos 2\frac{A_u\pi}{an+1},$$

où, dans le premier membre, il faut intégrer entre les limites

$$x = 0,\ x = an + 1,$$

et dans le second, entre les limites

$$u = 1,\ u = n + 1;$$

on aura semblablement, en intégrant entre les mêmes limites,

$$\Sigma \cos 2\frac{A_p x^a\pi}{an+1} = 1 + a\,\Sigma \cos 2\frac{A_u\pi}{an+1}.$$

Si à présent on ôte de la série

$$1,\ 2,\ 3,\ldots\ldots\ an,$$

les n nombres

$$A_1,\ A_2,\ A_3,\ldots\ldots\ A_n,$$

et que l'on prenne un nombre quelconque B_1 parmi les $(a-1)n$, nombres qui restent, on aura, en multipliant B_1 par

$$1^a,\ 2^a,\ 3^a,\ldots\ldots\ (na)^a,$$

une série de n nombres divers entre eux, et tous différents des nombres

$$A_1,\ A_2,\ A_3,\ldots\ldots\ A_n,$$

qui se répéteront a fois. Si l'on appelle

$$B_1,\ B_2,\ B_3,\ldots\ldots\ B_p,$$

ces nombres, en multipliant l'un quelconque B_p d'entre eux, par toutes les puissances a^{mes}

$$1^a,\ 2^a,\ 3^a,\ldots\ldots\ (nd)^a,$$

on aura de nouveau les nombres

$$B_1,\ B_2,\ B_3,\ldots\ldots\ B_n,$$

disposés dans un ordre quelconque, et répétés chacun a fois, de manière que l'on aura

$$\Sigma\left(\cos 2\frac{B_p x^a \pi}{an+1} + \sqrt{1}\sin 2\frac{B_p x^a \pi}{an+1}\right)$$
$$= 1 + n\,\Sigma\left(\cos 2\frac{B_u \pi}{an+1} + \sqrt{1}\sin 2\frac{B_u \pi}{an+1}\right),$$

en intégrant entre les limites

$$x = 0,\ x = an+1;\ u = 1,\ u = n+1.$$

On pourrait de même obtenir les séries

$$C_1,\ C_2,\ C_3,\ldots\ldots\ C_n,$$
$$D_1,\ D_2,\ D_3,\ldots\ldots\ D_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$R_1,\ R_2,\ R_3,\ldots\ldots\ R_n,$$

toutes composées de n termes divers. Le nombre de toutes les séries que nous avons considérées serait a, de manière qu'en réunissant tous les termes qu'elles contiennent, et en les rangeant d'après leur ordre de grandeur, on aurait la série des nombres naturels

$$1,\ 2,\ 3,\ 4,\ldots\ldots\ \ an.$$

Il serait aisé de démontrer que, parmi les a séries que nous avons trouvées, il en existe un nombre b (qui est égal au nombre des entiers plus petits que a, et qui n'ont pas de commun diviseur avec a) de la forme

$$\begin{aligned} &E_1,\ E_2,\ E_3,\ldots\ldots\ \ E_n,\\ &F_1,\ F_2,\ F_3,\ldots\ldots\ \ F_n; \end{aligned}$$

et telles que si l'on multiplie un terme quelconque E_p de l'une d'entre elles, par tous les termes de la même série

$$(23)\qquad A_1,\ A_2,\ A_3,\ldots\ldots\ \ A_n,$$

on aura de nouveau la série

$$E_1,\ E_2,\ E_3,\ldots\ldots\ \ E_n;$$

Si l'on multiplie la suite (23) par E_p^2, ou aura une autre des séries trouvées, et à chaque puissance de E_p on aura une nouvelle série; mais cela est étranger à notre but.

A présent nous supposerons, pour abréger, que l'on fasse

$$\begin{aligned} &\Sigma\left(\cos 2\frac{A_p\pi}{an+1}+\sqrt{1}\sin 2\frac{A_p\pi}{an+1}\right)^{x}\\ &=1+n\,\Sigma\left(\cos 2\frac{A_u\pi}{an+1}+\sqrt{1}\sin 2\frac{A_u\pi}{an+1}\right)=1+nA;\\ &\Sigma\left(\cos 2\frac{B_p\pi}{an+1}+\sqrt{-1}\,1\sin 2\frac{Bp\pi}{an+1}\right)^{x}\\ &=1+n\,\Sigma\left(\cos 2\frac{B_u\pi}{an-1}+\sqrt{-1}\sin 2\frac{B_u\pi}{an+1}\right)=1+n\,B;\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

et en général

$$\begin{aligned} &\Sigma\left(\cos 2\frac{R_p\pi}{ad+1}+\sqrt{-1}\sin 2\frac{R_p\pi}{an+1}\right)^{x}\\ &=1+n\,\Sigma\left(\cos 2\frac{R_u\pi}{an+1}+\sqrt{-1}\sin 2\frac{R_u\pi}{an+1}\right)=1+n\,R; \end{aligned}$$

en intégrant entre les limites

$$x = 0, \quad x = an + 1,$$
$$u = 1, \quad u = n + 1.$$

Si l'on avait à résoudre la congruence

$$x^a + 1 \equiv 0 \qquad [\text{mod. } an + 1],$$

on sait, d'après ce que nous avons dit, que le nombre N_1 de ses solutions sera exprimé par la formule

$$(an+1)N_1 = \begin{cases} \Sigma\left(\cos\frac{0\pi}{an+1} + \sqrt{-1}\sin\frac{0\pi}{an+1}\right)^{x^a+1} \\ + \Sigma\left(\cos\frac{2\pi}{an+1} + \sqrt{-1}\sin\frac{2\pi}{an+1}\right)^{x^a+1} \quad \ldots. \\ + \Sigma\left(\cos 2\frac{an\pi}{an+1} + \sqrt{-1}\sin 2\frac{an\pi}{an+1}\right)^{x^a+1} \end{cases}$$

$$= an + 1 +$$
$$\left(\cos\frac{2\pi}{an+1} + \sqrt{-1}\sin 2\frac{\pi}{an+1}\right)\Sigma\left(\cos 2\frac{x^a\pi}{an+1} + \sqrt{-1}\sin 2\frac{x^a\pi}{an+1}\right) + \text{etc.},$$

où il faut intégrer entre les limites

$$x = 0, \quad x = an + 1.$$

En distribuant par groupes les multiples de l'arc

$$1, \ 2, \ 3, \ldots\ldots \ an,$$

comme nous l'avons indiqué, et en représentant ces groupes par des lettres, comme nous l'avons déjà fait, on aura

$$(an+1)N_1 = 1 + an + A(1 + nA)$$
$$+ B(1 + nB) \ldots\ldots\ldots + R(1 + nR).$$

De même le nombre N_2 des solutions de la congruence

$$x^a + y^a + 1 \equiv 0 \qquad [\text{mod. } an + 1]$$

serait donné par l'équation

$$(1+an)\,N_2 = \Sigma\left(\cos\frac{0\pi}{an+1}+\sqrt{-1}\sin\frac{0\pi}{an-1}\right)^{x^a+y^a+1}$$
$$+\,\Sigma\left(\cos\frac{2\pi}{an+1}+\sqrt{-1}\sin\frac{2\pi}{an+1}\right)^{x^a+y^a+1}+\text{etc.},$$
$$=(an+1)^2+A(1+nA)^2$$
$$+B(1+nB)^2.\ldots\ldots\quad+R(1+nR)^2,$$

en intégrant entre les limites

$$x=y=0,\quad x=y=an+1,$$

et on pourrait avoir de même le nombre des solutions des congruences

$$\left.\begin{array}{l} x^a+y^a+z^a+1\equiv 0 \\ x^a+y^a+z^a+u^a+1\equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}\end{array}\right\}\ldots\ldots\quad[\text{mod. } an+1]$$

jusqu'à la congruence à $a-1$ inconnues, qui donnerait

$$(1+an)\,N_{a-1} = (1+an)^{a-1}+A(1+nA)^{a-1}$$
$$+B(1+nB)^{a-1}\ldots\ldots\ldots+R(1+nR)^{a-1}.$$

En ajoutant à ces $a-1$ équations, l'équation connue

$$1+A+B+C.\ldots\ldots+R=0,$$

on aura a équations et a inconnues, et on pourra, par l'élimination, déterminer toutes les quantités

$$A,\ B,\ C,\ldots\ldots\quad R.$$

Au lieu de faire cette élimination, il sera plus aisé de chercher une équation

$$(24).\ldots\ldots\quad z^a+q_1\,z^{a-1}+q_2\,z^{a-2}.\ldots\ldots\quad+q_a=0,$$

dont les a racines soient les quantités

$$A,\ B,\ C,\ldots\ldots\quad R:$$

les coefficients de cette équation se détermineront avec la plus grande facilité, puisqu'on déduit des équations que nous avons trouvées précédemment

$$A + B + C..... + R = -1,$$

$$A^2 + B^2 + C^2..... + R^2 = \frac{(N_1-1)(an+1)+1}{n}$$

$$..... \text{ etc.}$$

équations qui fournissent en général la somme des puissances r^{mes} des quantités

$$A, B, C,..... R.$$

On voit donc que, pour trouver les quantités

$$A, B, C,..... R,$$

on a une équation de l'a^{me} degré; et si $Z = Q$ est l'expression générale des racines de l'équation (24), on trouvera toujours, en appelant r l'une des racines de

$$\frac{x^{an+1}-1}{x-1} = 0,$$

l'équation

$$r^{A_1} + r^{A_2} + r^{A_3} ..... + r^{A_n} = Q,$$

et par suite l'équation

$$X_1 = x^{A_1} + x^{A_2} + x^{A_3} ..... + x^{A_n} - Q = 0,$$

aura n racines communes avec l'autre

$$X = \frac{x^{an+1}-1}{x-1} = 0.$$

Donc en cherchant le plus grand diviseur commun entre X et X_1, on aura une équation du degré n, qui aura pour racines les quantités

$$r^{A_1}; r^{A_2}, r^{A_3} ..... r^{A_n},$$

et qui sera de la forme

$$X_2 = x^n + \alpha x^{n-1} + \zeta x^{n-2} + \gamma x^{n-3} \ldots + \varepsilon = 0;$$

et comme il y a a valeurs de Q, on aura a équations semblables à l'équation $X_2 = 0$, toutes du degré a, et telles que leur produit formera l'équation

$$\frac{x^{an+1}-1}{x-1} = 0.$$

Donc enfin:

« Étant proposée l'équation

$$\frac{x^{an+1}-1}{x-1} = 0,$$

« dans laquelle $an+1$ est un nombre premier, on pourra toujours « la décomposer en a équations du degré n, au moyen d'une équa- « tion du degré a. »

On voit que ce théorème renferme toute la théorie de M. Gauss sur la résolution des équations à deux termes. Nous ne nous arrêterons pas à démontrer le complément de cette théorie, c'est-à-dire que toute équation (24) peut se réduire à une autre équation du même degré, de la forme

$$Z_1^a - b = 0.$$

Cela nous mènerait trop loin, et d'ailleurs il n'est pas difficile d'y suppléer de soi-même.

En traitant de nouveau l'équation $X_2 = 0$, avec une méthode semblable à celle que nous venons d'exposer, on pourrait la décomposer encore en d'autres équations, et réduire enfin l'équation proposée

$$x^{an+1} - 1 = 0,$$

à plusieurs équations dont les degrés fussent tous les nombres premiers qui divisent an.

En partant du même principe, on peut résoudre d'autres équations algébriques, et notamment celles d'où dépend la division de la lemniscate en parties égales (voyez la note IV^e), et trouver les valeurs de

$$\sum_{x=0}^{x=n} \cos 2\frac{ax^m\pi}{n}, \qquad \sum_{x=0}^{x=n} \cos 2\frac{a(x^m+\delta)\pi}{n}, \text{ etc.},$$

qu'il serait bien difficile d'avoir en faisant usage des méthodes connues pour calculer les intégrales définies. Notre méthode s'applique aussi à la résolution d'une congruence quelconque

$$x^m - a \equiv 0 \qquad [\text{mod. } n];$$

mais il nous paraît que les applications que nous avons exposées de l'équation (10) trouvée au commencement suffisent pour démontrer qu'elle renferme la théorie des congruences dans toute sa généralité.

Dans un mémoire que nous avons eu l'honneur de présenter précédemment à l'Académie, nous avons exposé une formule qui donne toujours, en nombres et en termes finis, la somme des diviseurs d'un nombre quelconque. Cette formule a été trouvée en considérant la somme des puissances n^{mes} des racines de l'équation

$$(x-1)\ (x^2-1)\ (x^3-1)\ldots\ldots \qquad (x^n-1)=0;$$

si l'on cherchait la somme des puissances n^{mes} des racines de l'équation

$$(x-y)\ (x^2-y)\ (x^3-y)\ldots\ldots \quad (x^m-y)\ldots\ldots \quad \text{etc.} = 0,$$

on pourrait trouver un nombre premier plus grand qu'une limite donnée, directement et sans tâtonnement. Mais nous ne pouvons pas exposer à présent le résultat de nos recherches sur ce sujet,

et nous réservons cela pour une autre occasion. Le but que nous nous étions proposé dans ce mémoire était de montrer de quelle manière on pouvait déduire directement de notre théorie, et d'une seule formule, tous les résultats qu'on avait trouvés avec beaucoup de difficultés, et par des méthodes très-différentes, sur les congruences; et nous osons nous flatter que l'Académie voudra accueillir avec indulgence l'essai que nous avons l'honneur de lui présenter.

NOTES.

NOTE I.

La formule de M. de Laplace pour exprimer les coefficients A_1, A_2, A_3 et A_n dans le développement de

$$\frac{1}{e^u-1} = \frac{1}{u} + A_1u + A_2u^2 + A_3u^3 + \text{etc.} \ldots + A_nu^{n-1}$$

est d'une application infiniment pénible lorsque n est un nombre un peu grand; et d'ailleurs elle donne $A_1 = \infty$, au lieu de $A_1 = -\frac{1}{2}$ comme on doit avoir. La formule que nous avons donnée dans les mémoires de Turin pour développer les polynomes est beaucoup plus simple et s'applique avec facilité.

En effet, nous avons trouvé pour le polynome

$$(1 + a_1u + a_2u^2 \ldots + a_nu^n + \text{etc.})^m = 1 + A_1u + A_2u^2 \ldots + A_nu^n + \text{etc.}$$

l'expression

$$A_n = \begin{cases} \dfrac{nma_n}{n} + ((n-1)m-1)\dfrac{a_{n-1}}{n}(ma_1) \\ + ((n-2)m-2)\dfrac{a_{n-2}}{2}\left(\dfrac{2ma_2 + (m-1)a_1(ma_1)}{2}\right) \\ \ldots\ldots\ldots\ldots\ldots \\ + ((n-t)m-t)\dfrac{a_{n-t}}{n}\left(\dfrac{tma_t + ((t-1)m-1)a_{t-1}(ma_1) + \text{etc.}}{t}\right) \\ \ldots\ldots\ldots\ldots \text{etc.} \end{cases}$$

et puisque l'on a

$$\frac{1}{e^u-1} = \frac{1}{u + \frac{u^2}{1.2} + \frac{u^3}{1.2.3} \ldots + \frac{u^n}{1.2.3\ldots n} + \text{etc.}}$$

$$= \frac{1}{u}\left(\frac{1}{1 + \frac{u}{1.2} + \frac{u^2}{1.2.3} \ldots + \frac{u^{n-1}}{1.2.3\ldots n} + \text{etc.}}\right)$$

en comparant le polynome

$$\frac{1}{1+\frac{u}{1.2}+\frac{u^2}{1.2.3}\ldots.+\frac{u^{n-1}}{1.2.3\ldots n}+\text{etc.}}$$

à l'autre

$$(1+a_1 u+a_2 u^2 \ldots\ldots+a_n u^n+\text{etc.})^m,$$

on aura

$$m=-1,\ a_1=\frac{1}{1.2},\ a_2=\frac{1}{1.2.3},\ \ldots\ a_n=\frac{1}{1.2.3\ldots(n+1)},$$

et par conséquent, en substituant ces valeurs dans celles de A_n, on obtiendra

$$A_n=\frac{-1}{1.2.3\ldots.(n+1)}-\frac{1}{1.2.3\ldots..n}\left(\frac{-1}{1.2}\right)$$
$$-\frac{1}{1.2.3\ldots.(n-1)}\left(\frac{-1}{1.2.3}-\frac{1}{1.2}\left(\frac{-1}{1.2}\right)\right)$$
$$-\frac{1}{1.2.3\ldots(n-t)}\left(\frac{-1}{1.2.3\ldots(t+2)}-\frac{1}{1.2.3\ldots(t+1)}\left(\frac{-1}{1.2}\right)-\text{etc.}\right)-\text{etc.}$$

En faisant dans cette formule successivement $n=1, 2, 3, \ldots$ etc., on aura

$$A_1=\frac{-1}{2},\ A_2=\frac{-1}{6}+\frac{1}{4}=\frac{1}{12},$$
$$A_3=\frac{-1}{24}+\frac{1}{12}+\frac{1}{12}-\frac{1}{8}=0,\ \text{etc.}$$
$$\ldots\ldots\ \text{etc.}$$

NOTE II.

Etant données deux équations en y, l'une du degré n, et l'autre du degré m, si on élimine y on aura l'équation

$$1+\Sigma\left(\frac{P_t A_{t-1}}{2}+\Sigma\frac{P_{t_x} A_{t_x-1}}{t_x}\left[\frac{P_{t_{x-1}}-t_x A_{t_{x-1}-t_x-1}}{t_{x-1}}\right]^x\right)=0,$$

(en intégrant entre les limites

$$t = 1,\ t = mn + 1,$$
$$x = 1,\ x = t,\ t_u = x - u + 1,\ t_u = t_{u-1},$$

et en faisant $t_0 = t$), dans laquelle P_r exprime en général la somme des puissances r^{mes} des racines d'une équation donnée, et A_v représente le coefficient de la puissance v^{mes} : du développement connu du polynome.

On obtiendra de même dans l'équation

$$(1 + a_1 x + a_2 x^2 \ldots + a_n x^n + \text{etc.})^m = 1 + A_1 x + A_2 x^2 \ldots + A_n x_n + \text{etc.}$$

$$A_n = ma_n + m \Sigma a_{n_v} e^{\Sigma log\left((n_v - n_{v+1})m - n_{v+1}\right) \frac{a_{n_v - n_{v+1}}}{n_v}};$$

e étant la base des logarithmes hyperboliques, et les intégrations étant effectuées entre les limites

$$v = 0,\ v = u,$$
$$u = 1,\ u = n,$$
$$u_p = u - p + 1,\ n_p = n_{p-1}.$$

La somme des puissances n^{mes} des racines de l'équation

$$x^n - a_1 x^{n-1} - a_2 x^{n-2} \ldots\ldots - a_n = 0,$$

est donnée par la formule

$$P_m = ma_m + \Sigma (m - m_1) a_{m_u} e^{\Sigma log\, a_{m_s - m_{s+1}}}$$

où il faut intégrer entre les limites

$$s = 0,\ s = u;\ m_p = u + 1 - p,\ m_p = m_{p-1};$$
$$u = 1,\ u = m;$$

et faire $m_0 = m$, comme auparavant.

Il y a deux ans que nous avons trouvé ces formules, dont nous avons donné une application dans un mémoire présenté à l'Académie royale des sciences de Paris, en janvier 1824, en cherchant la somme des diviseurs d'un nombre quelconque. Elles ont l'avantage de n'exiger aucune opération analytique pour être appliquées, car il suffit d'y substituer les coefficients connus

$$a_1,\ a_2,\ a_3, \ldots\ldots a_n, \text{ etc.}$$

pour en avoir la valeur pour chaque cas particulier; de plus, lorsque le coefficient général a_n est une fonction donnée de n, on peut les transformer en intégrales définies et en obtenir la valeur directement en nombres; ce qui est d'un grand avantage dans la théorie des nombres. M. Cauchy nous a montré un mémoire inédit dans lequel il expose des formules propres à exprimer les

fonctions symétriques; mais ses formules sont tout à fait différentes des nôtres, et d'ailleurs elles exigent des différentiations successives, tandis que nos expressions ne demandent aucune opération préliminaire.

NOTE III.

Soit proposé, par exemple, de résoudre en nombres entiers et positifs l'équation

$$3x + 1 = 4y,$$

si on la compare avec l'autre

$$ax + b = cy,$$

qui donne

$$(a) \qquad x = \frac{c-1}{2} + \frac{1}{2} \sum_{y=1}^{y=c} \frac{\sin (2b-a)\frac{y\pi}{c}}{\sin \frac{ay\pi}{c}}$$

on aura $a = 3$, $b = 1$, $c = 4$, et par conséquent

$$x = \frac{3}{2} + \frac{1}{2}\left(\frac{-\sin\frac{\pi}{4}}{\sin\frac{3\pi}{4}} - \frac{\sin\frac{2\pi}{4}}{\sin\frac{6\pi}{4}} - \frac{\sin\frac{3\pi}{4}}{\sin\frac{9\pi}{4}} \right)$$

$$= \frac{3}{2} + \frac{1}{2}(-1+1-1) = \frac{3}{2} - \frac{1}{2} = 1,$$

et la valeur $x = 1$ résoudra l'équation proposée, comme il est facile de voir.

Il est clair que l'on aura aussi

$$x = \frac{c}{2} + \frac{1}{2} \sum_{y=1}^{y=c} \sin \frac{2by\pi}{c} \cot \frac{ay\pi}{c}$$

en développant le second membre de l'équation (a).

Ces formules pourraient être généralisées, et il serait aisé de les étendre aux degrés supérieurs des congruences; mais on aurait alors des expressions plus compliquées.

En général, les valeurs de x de l'équation (a) peuvent être calculées au moyen des tables des sinus, car de cette manière on aura une valeur très-approchée de

x, et comme x doit être un nombre entier, on prendra pour sa valeur exacte le nombre entier le plus approché,

NOTE IV.

Soit proposée l'équation $x^n - 1 = 0$, et soit s une racine primitive du nombre premier n: si l'on exprime par $r_1, r_2, \ldots r_{n-1}$, les $n-1$ racines de l'équation $\frac{x^n-1}{x-1} = 0$, il est clair qu'on aura

$$r_2 = r_1^s, \; r_3 = r_2^s, \; r_4 = r_3^s, \; \ldots \text{ etc.};$$

maintenant si l'on suppose que l'équation $x^m + a_1 x^{m-1} r^m \ldots + a_m = 0$, ait les m racines $r_1, r_2, \ldots$ telles qu'en exprimant par $\varphi(y)$ une fonction rationnelle quelconque de y, on ait toujours $r_2 = \varphi(r_1)$, $r_3 = \varphi(r_2)$ ..... etc., on pourra encore résoudre complétement l'équation $x^m + a_1 x^{m-1} \ldots\ldots + a_m = 0$, (lorsqu'elle n'a pas de facteurs rationnels) en employant la même méthode dont Lagrange s'est servi dans les notes de la 2e édition de la Résolution des équations numériques, pour résoudre l'équation à deux termes.

ADDITION.

Dans un mémoire présenté précédemment à l'Académie, nous avons énoncé ce théorème :

« Qu'un nombre quelconque positif est la somme de quatre cubes rationnels et « positifs. »

En voici la démonstration.

Soit M un nombre positif, et q un nombre rationnel, on aura toujours l'identité

$$(b) \qquad M = \left(\frac{M + 48q^3}{24q^2}\right)^3 + \left(\frac{M - 48q^3}{24q^2}\right)^3 - \left(\frac{M}{24q^2}\right)^3 - \left(\frac{M}{24q^2}\right)^3,$$

(comme il est facile de s'en assurer en développant) qui prouve qu'un nombre quelconque est la somme de quatre cubes rationnels; mais d'après l'énoncé du théorème, ces cubes doivent être positifs, et ils ne le sont pas dans l'équation (b): voyons comment on peut les réduire tels.

Puisque q est un nombre quelconque, nous supposerons q positif, et $M > 48q^3$, ce qui rendra positif les deux premiers cubes du second membre de l'équation (b), tandis que les deux autres seront toujours négatifs. A présent il faut observer que dans l'identité

$$(c) \qquad a^3 - b^3 = a^3\left(\frac{a^3-2b^3}{a^3+b^3}\right)^3 + b^3\left(\frac{2a^3-b^3}{a^3+b^3}\right)^3$$

si l'on a $a^3 > 2b^3$, on aura encore $2a^3 > b^3$, et par conséquent le second membre sera composé de deux cubes positifs dont la somme sera égale à la différence des deux cubes donnés a^3 et b^3. Si nous faisons

$$a^3 = \left(\frac{M+48q^3}{24q^3}\right)^3, \quad b^3 = \left(\frac{M}{24q^3}\right)^3,$$

l'équation (c) se transformera en celle-ci

$$\left(\frac{M+48q^3}{24q^3}\right)^3 - \left(\frac{M}{24q^3}\right)^3$$

$$= \left(\frac{M+48q^3}{24q^3}\right)^3 \left(\frac{\left(\frac{M+48q^3}{24q^3}\right)^3 - 2\left(\frac{M}{24q^3}\right)^3}{\left(\frac{M+48q^3}{24q^3}\right)^3 + \left(\frac{M}{24q^3}\right)^3}\right)^3$$

$$+ \left(\frac{M}{24q^3}\right)^3 \left(\frac{2\left(\frac{M+48q^3}{24q^3}\right)^3 - \left(\frac{M}{24q^3}\right)^3}{\left(\frac{M+48q^3}{24q^3}\right)^3 + \left(\frac{M}{24q^3}\right)^3}\right)^3$$

$$= \left(\frac{M+48q^3}{24q^3}\right)^3 \left(\frac{(M+48q^3)^3 - 2M^3}{(M+48q^3)^3 + M^3}\right)^3$$

$$+ \left(\frac{M}{24q^3}\right)\left(\frac{2(M+48q^3)^3 - M^3}{(M+48q^3)^3 + M^3}\right) \qquad \ldots\ldots (d)$$

Il est clair que si l'on suppose $(M+48q^3)^3 > 2M^3$, les deux cubes du second membre seront positifs : nous supposerons pour le moment cette condition remplie, et nous considérerons de nouveau l'identité (c) en prenant

$$a^3 = \left(\frac{M+48q^3}{24q^3}\right)^3 \left(\frac{(M+48q^3)^3 - 2M^3}{(M+48q^3)^3 + M^3}\right)^3, \quad b = \left(\frac{M}{24q^3}\right)^3;$$

en substituant ces valeurs dans l'identité (c) nous aurons

$$\left(\frac{M+48q^3}{24q^3}\right)^3 \left(\frac{(M+48q^3)^3 - 2M^3}{(M+48q^3)^3 + M^3}\right)^3 - \left(\frac{M}{24q^3}\right)^3 =$$

$$= \left(\frac{M+48q^3}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 \times$$

$$\times \left(\frac{\left(\frac{M+48q^3}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 - 2\left(\frac{M}{24q^2}\right)^3}{\left(\frac{M+48q^3}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 + \left(\frac{M}{24q^2}\right)^3} \right)^3$$

$$+ \left(\frac{M}{24q^2}\right)^3 \left(\frac{2\left(\frac{M+48q^3}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 - \left(\frac{M}{24q^2}\right)^3}{\left(\frac{M+48q^3}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 + \left(\frac{M}{24q^2}\right)^3} \right)^3 \quad \ldots . (d)$$

le premier terme du second membre de cette équation peut s'écrire encore de la manière suivante

$$\left(\frac{48q^3+M}{24q^2}\right)^3 \left(\frac{(M+48q^3)^3-2M^3}{(M+48q^3)^3+M^3}\right)^3 \times$$

$$\times \left(\frac{(48q^3+M)^3\,((48q^3+M)^3-2M^3)^3-2M^3\,((48q^3+M^3)^2+M^3)^3}{(48q^3+M)^3\,((48q^3+M)^3-2M^3)^3-2M^3\,((48q^3+M^3)^3+M^3)^3} \right)^3,$$

et l'on voit que si ce premier cube est positif, le second le sera encore (dans l'hypothèse que $(M+48q^3)^3 > 2M^3$); à présent pour le rendre positif, il faut et il suffit que l'on ait

$$(e) \qquad (48q^3+M^3)^3\,((48q^3+M)^3-2M^3)>2M^3)\,(48q^3+^3+M^3)^3$$

et cette condition renferme l'autre que nous avons supposée $(48q^3+M)^3 > 2M^3$; ainsi lorsque l'inégalité (e) sera satisfaite, celle-ci $(48q^3+M)^3 > 2M^3$ le sera aussi si nous faisons $48q^3 = z$, l'inégalité (e) se transformera dans celle-ci

$$(z+M)\,((z+M)^3-2M^3)-M\,((z+M)^3+M^3)\sqrt[3]{2}>0$$

laquelle étant développée donne

$$(z+M)\,(z^3+3z^2M+3zM^2-M^3)+M\,(z^3+3z^2M+3zM^2+2M^3)\sqrt[3]{2}$$
$$=z^4+4z^3M+6z^2M^2+2zM^3-M^4-2M^4\sqrt[3]{2}-3zM^3\sqrt[3]{2}-3z^2M^2\sqrt[3]{2}-z^3M^2\sqrt[3]{2}$$
$$=z^4+z^3M\,(4-\sqrt[3]{2})+z^2M^2\,(6-3\sqrt[3]{2})+zM^3\,(2-3\sqrt[3]{2})-M^4\,(1+2\sqrt[3]{2})>0 \quad \ldots . (f)$$

Nous avons supposé que $M > 48q^3$, ou bien $M > z$; en faisant donc $M = Az$, on aura $A>1$: si l'on substitue cette valeur de M dans l'inégalité (f), et qu'on la divise par z^4, on aura

$$1+A\,(4-\sqrt[3]{2})+A^2\,(6-3\sqrt[3]{2})+A^3\,(2-3\sqrt[3]{2})-A^4(1+2\sqrt[3]{2})>0:$$

si l'on fait à présent $A = 1+\omega$, on obtiendra $\ldots . (g)$

$$\ldots . 1+(4-\sqrt[3]{2})\,(1+\omega)+(6-3\sqrt[3]{2})(1+\omega)^2+(2-3\sqrt[3]{2})(1+\omega)^3-(1+2\sqrt[3]{2})\,(1+\omega)^4,$$
$$=(12-9\sqrt[3]{2}+\omega\,(18-24\sqrt[3]{2})+\omega^2(6-24\sqrt[3]{2})-\omega^3\,(2+11\sqrt[3]{2})-\omega^4(1+2\sqrt[3]{2}))>0,$$

je dis que l'on pourra toujours satisfaire à cette inégalité en prenant pour ω un nombre rationnel et positif. En effet puisque $\frac{126}{100} > \sqrt[3]{2}$, on aura

$$12 - 9\sqrt[3]{2} > 12 - \left(\frac{126}{100} \times 9 = \frac{1200 - 1134}{100} = \frac{66}{100} \right)$$

ou bien

$$12 - 9\sqrt[3]{2} > \frac{33}{50};$$

et ω devra être un nombre tel que la somme de tous les termes qu'il multiplie dans l'inégalité (g), soit moindre que $\frac{33}{50}$: nous prendrons partout $\frac{126}{100}$ pour valeur de $\sqrt[3]{2}$ sans crainte d'erreur, parce que dans l'inégalité (g) tous les termes, moins les premiers sont négatifs, et nous devrons avoir

$$\frac{33}{50} - \omega\left(24 \times \frac{126}{100} - 18 \right) - \omega^2\left(24 \times \frac{126}{100} - 6 \right) - \omega^3\left(11 \times \frac{126}{100} + 2 \right) - \omega^4\left(2 \times \frac{126}{100} + 1 \right)$$

$$= \frac{33}{50} - \omega\left(\frac{3024 - 1800}{100} \right) - \omega^2\left(\frac{3024 + 600}{100} \right) - \omega^3\left(\frac{1386 + 200}{100} \right) - \omega^4\left(\frac{252 + 100}{100} \right);$$

$$\frac{33}{50} - \frac{612}{50}\omega - \frac{1212}{50}\omega^2 - \frac{793}{50}\omega^3 - \frac{176}{50}\omega^4 > 0$$

d'où, en multipliant par 50, nous déduirons

$$(h) \qquad 33 - 612\omega - 1212\omega^2 - 793\omega^3 - 176\omega^4 > 0;$$

si l'on fait $\omega = \frac{1}{\rho}$, et que l'on multiplie tous les termes par $\frac{\rho^4}{33}$, on obtiendra

$$\rho^4 - \frac{612}{33}\rho^3 - \frac{1212}{33}\rho^2 - \frac{793}{33}\rho - \frac{226}{33} > 0.$$

Cette dernière inégalité sera satisfaite en prenant $\rho > \frac{1212}{33} + 1$, ou bien

$$\rho = \frac{1245}{33} + u = \frac{415}{11} + u = \frac{415 + 11u}{11};$$

et par conséquent l'inégalité (h) sera satisfaite en prenant

$$\omega = \frac{11}{415+11u}; \quad \omega < \frac{11}{415},$$

u étant un nombre quelconque rationnel et positif. Mais puisque l'on a

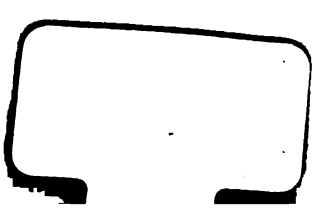
$$M = As = (1+\omega)\,s = \left(1+\frac{11}{415+11u}\right)s$$

$$= \left(\frac{426+11u}{415+11u}\right)s = 48q^3\left(\frac{426+11u}{415+11u}\right),$$

on aura aussi

$$q^3 = \frac{M}{48}\left(\frac{415+11u}{426+11u}\right).$$

On devra par conséquent prendre pour q^3 un cube rationnel positif compris entre $\frac{M}{48}$ et $\left(\frac{415+11u}{426+11u}\right)\frac{M}{48}$ ou bien entre $\frac{M}{48}$ et $\frac{415}{426}\frac{M}{48}$; et l'on voit qu'il existera toujours un nombre infini de ces cubes. A présent si l'on substitue l'un de ces cubes dans les identités (c), (d), on aura décomposé le nombre M en quatre cubes rationnels et positifs.

Ce théorème offre le premier exemple de la décomposition des nombres en puissances d'un degré plus élevé que le deuxième : on pourrait le généraliser et en déduire plusieurs autres propositions nouvelles.

IMPRIMERIE ROYALE. — Septembre 1833.